NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FIGHTING DARK NETWORKS: USING SOCIAL NETWORK ANALYSIS TO IMPLEMENT THE SPECIAL OPERATIONS TARGETING PROCESS FOR DIRECT AND INDIRECT APPROACHES

by

Matthew D. Erlacher

March 2013

Thesis Advisor: Sean F. Everton
Co-Advisor Dorothy E. Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington, DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE FIGHTING DARK NETWORKS: USING SOCIAL NETWORK ANALYSIS TO IMPLEMENT THE SPECIAL OPERATIONS TARGETING PROCESS FOR DIRECT AND INDIRECT APPROACHES			**5. FUNDING NUMBERS**
6. AUTHOR(S) Matthew D. Erlacher			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Since the September 11, 2001, terrorist attacks, the United States military has been engaged against transnational networks, a domain for which many of its processes were not designed and are not well-suited. A significant part of the military's struggle of the last decade of war has been a lack of a framework for understanding and measuring changes in social networks, especially insurgent or terrorist networks known as dark networks. This thesis puts forth an experimental framework called the Special Operations Network Analysis Process, or SONAP, to solve that problem. SONAP combines the CARVER target analysis method with Social Network Analysis and a systems framework for identifying and bounding social mechanisms that support dark networks, as well as a means for identifying and evaluating changes in networks. This framework is then applied to a 2006 open-source data set of an Indonesian terrorist network. The result is a demonstrated utility in not only understanding the structure of that dark network, but also in designing an intervention strategy, along with means to measure structural and operational changes in that network.

14. SUBJECT TERMS social network analysis, dark networks, special operations, irregular warfare, targeting, direct approach, indirect approach, terrorism, counterterrorism, counterinsurgency, pseudo operations, effects-based operations, effects-based thinking, systems thinking, social systems			**15. NUMBER OF PAGES** 193
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

FIGHTING DARK NETWORKS: USING SOCIAL NETWORK ANALYSIS TO IMPLEMENT THE SPECIAL OPERATIONS TARGETING PROCESS FOR DIRECT AND INDIRECT APPROACHES

Matthew D. Erlacher
Major, United States Army
B.S., United States Military Academy, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
March 2013

Author: Matthew D. Erlacher

Approved by: Sean F. Everton
Thesis Advisor

Dorothy E. Denning
Thesis Co-Advisor

John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Since the September 11, 2001, terrorist attacks, the United States military has been engaged against transnational networks, a domain for which many of its processes were not designed and are not well-suited. A significant part of the military's struggle of the last decade of war has been a lack of a framework for understanding and measuring changes in social networks, especially insurgent or terrorist networks known as dark networks. This thesis puts forth an experimental framework called the Special Operations Network Analysis Process, or SONAP, to solve that problem. SONAP combines the CARVER target analysis method with Social Network Analysis and a systems framework for identifying and bounding social mechanisms that support dark networks, as well as a means for identifying and evaluating changes in networks. This framework is then applied to a 2006 open-source data set of an Indonesian terrorist network. The result is a demonstrated utility in not only understanding the structure of that dark network, but also in designing an intervention strategy, along with means to measure structural and operational changes in that network.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADP	Army Doctrinal Publication
ADRP	Army Doctrinal Reference Publication
AOB	Advance Operating Base
CARVER	Criticality, Vulnerability, Recuperability, Vulnerability, Effects, Recognizability
CCRP	Command and Control Research Program
CIA	Central Intelligence Agency
COG	Center of Gravity
CORDS	Civil Operations and Revolutionary Development Support
CT	Counterterrorism
D3A	Detect, Decide, Deliver, Assess
DIME	Diplomatic, Information, Military and Economic
DoD	Department of Defense
EBA	Effects-Based Approach
EBO	Effects-Based Operations
F3EAD	Find, Fix, Finish, Exploit, Analyze, Disseminate
FM	Field Manual
GCC	Geographic Combatant Command
HUMINT	Human Intelligence
HVI	High-Value Individual
ICG	International Crisis Group
IED	Improvised Explosive Device
IO	Information Operations
JFC	Joint Force Command
JFSOCC	Joint Force Special Operations Component Command
JI	Jema'ah Islamiyah
JP	Joint Publication
JSOTF	Joint Special Operations Task Force

KPP	Key Player Problem
KPP-Neg	Key Player Problem-Negative
KPP-Pos	Key Player-Problem-Positive
MISO	Military Information Support Operations
OSW	Open-Source Warfare
PMESII	Political, Military, Economic, Security, Intelligence, Information
PsyOp	Psychological Operations
SF	Special Forces
SFODA	Special Forces Operational Detachment-Alpha
SIGINT	Signals Intelligence
SNA	Social Network Analysis
SOF	Special Operations Forces
SONAP	Special Operations Network Analysis Process
SOTF	Special Operations Task Force
SOTP	Special Operations Targeting Process
TRADOC	Training and Doctrine Command
TSOC	Theater Special Operations Command
USSOCOM	United States Special Operations Command
ZANLA	Zimbabwe African National Liberation Army
ZIPRA	Zimbabwe People's Revolutionary Army

ACKNOWLEDGMENTS

First and foremost, I want to thank my wife for her love, patience, support and example in academia. I will live the rest of my life trying to live up to and returning the love she shows me every day. I want to thank my parents for instilling in me a spirit of determination, exploration, and learning–I still live it. I also thank them for their heart-aching support for me in joining the Army. And, though he will never read this thesis, I thank my grandfather for the many days and late nights of war stories and tears we shared in looking at what war does to us.

I sincerely thank my advisors, Dr. Sean Everton and Dr. Dorothy Denning, for their eternal patience, wisdom and support for this very long road I took to complete this work.

I also want to thank Dr. Gordon McCormick, Dr. John Arquilla, and Dr. Doowan Lee for the time they took from their busy days to counsel and mentor me. I cannot go without thanking Professor George Lober for his intervention that finally set me on the track to starting and completing my thesis. I have to thank Master Sergeant Andy Zybas, Brigadier General Dave Fox, Colonel Chris Conner and Colonel Chris Miller for their extremely positive influences upon my career decisions.

Lastly, I want to thank that long-since-forgotten project officer at USSOCOM whose actions were instrumental in establishing the relationship between that organization and the Naval Postgraduate School that created the Department of Defense Analysis. Without that guy, this thesis and many others would not be possible and Special Operations would not be what it is today.

De Oppresso Liber

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> If I had an hour to solve a problem and my life depended on the solution, I would spend the first 55 minutes determining the proper question to ask, for once I know the proper question, I could solve the problem in less than five minutes. –Albert Einstein[1]

For most of its history, and much of the foreseeable future, America has been and will be embroiled in increasingly complex foreign conflicts that involve significant portions or the whole of native societies. These are called "wars amongst the people."[2] Wars amongst the people directly involve populations and various political entities that are motivated and enabled by many simultaneous factors[3] and mobilized and resourced according to social structures.[4] Because of the primacy of these non-military factors, modern industrial militaries are not well-suited for war amongst the people.[5] A primary characteristic of modern conflict complexity is the deliberate secrecy surrounding group members' participation, resources, and activities that creates an informational cloak that makes their networks and activities difficult to distill from the surrounding society. Networks that are inherently illicit and necessarily secretive for survival, such as terrorist, insurgent, or organized crime networks, are known as dark networks.[6]

Fighting dark networks, a form of irregular warfare, is considerably different from conventional warfare between industrial state militaries. Conventional warfare involves massive formations of troops and machines dependent upon superior technology, firepower and significant, tailored logistical burdens unified in the sole purpose of destroying an opponent's military might and political will to fight through attrition of men, materials and psychological cohesion. Conventional warfare has been the basis for structuring our modern military organizational patterns, weapons procurement, our command and control methods and supporting technologies, and our analytical and operational methods. We have established hierarchical organizational and procedural models to maintain maximal control of information and actions. These organizational and doctrinal structures, and accompanying philosophies and technolgies, were never intended for anything other than conventional* war.[7] Thus, the American military is, as a whole, unprepared for irregular warfare. Irregular warfare, or IW, is the domain where dark networks reign.

Within the U.S. military, however, there is a little-known process that is much better suited to meet the challenge of fighting dark networks. The U.S. Army's Special Forces community, or SF, has a long and very successful history focused on influencing indigenous social structures and developing native military and paramilitary forces.[8] But even their deep cultural understanding via routine close contact with the native populations in conflict zones is not enough to be fully successful in wars amongst the people. SF have a process for analysis and intervention that possesses a frame that is moderately well-suited to wars amongst the people, though it was not created for that purpose. That process is called the Special Forces Target Analysis, which feeds the Special Operations Targeting Process. Unfortunately, it views the world as hierarchically-dependent and static systems employing linear and additive casual loops. And therein lies the shortcoming of the current model of analysis.

A better theoretical basis is in complexity theory, with systems theory and social network theory describing the basis of a new model using the tenets of SF Target Analysis. Complexity theory accounts for an organic structural and dynamically interactive set of relations and frames the world as a network of networks, which enables application of social network analysis, or SNA, of actors and relations between actors. Combine this "network of networks"[9]approach with a similar analogy, a "system of systems,"[10] and it becomes clear that these frames are similar enough to allow knowledge of the social aspect of current and future conflict environments to be extremely insightful and useful information for actors, such as the military, attempting to understand and intervene in foreign wars amongst the people using a blend of SNA and SF Target Analysis.

* This assessment includes the current U.S. Army and Marine Corps counterinsurgency manual, FM 3-24, and its joint military publication counterpart, JP 3-24. The current version (December, 2006) of the manual was written with Iraq (c. 2005) in mind, not as a generalized doctrine for universal applicability, though it has been applied in Afghanistan with poor effect.

A. PURPOSE

This thesis is intended to accomplish three things. First, it shows how the complexity of war amongst the people—specifically, warfare against dark networks—highlights a critical shortcoming in our military capabilities. Second, it describes and stitches together the Special Operations Targeting Process, specifically SF Target Analysis, and SNA, showing how the combined methodology offers not only conceptualizations of the environment, but also an improved methodology for framing, describing, analyzing and proscribing solutions in complex social conflict environments. Lastly, this thesis tests the usefulness of this hybrid methodology using an unclassified dataset, highlighting this type of analysis and then deriving an intervention strategy from that analysis. This methodology distills key players and mechanisms from a complex environment and enables micro-analysis of those key players and mechanisms for intervention according to the intent and information requirements of a chosen intervention method.

B. BACKGROUND

In spite of a long history of engaging in irregular warfare, warfare in the 21st century has proved to be radically different from what the American military had envisioned or prepared. Warfare continues to evolve. The Jominan and Clausewitzian traditions of warfare thought has not culminated in a doctrine that is well-suited to the social context wars amongst the people.[11] In order to fight the current conflicts in Afghanistan and Iraq, the American military has paved a major tangent to its attrition warfare tradition in an attempt to meet the enemy in the correct domain: war amongst the people. Yet, in spite of twice moving toward an appropriate counterinsurgency doctrine and array of supporting tactics while in conflict, first under the Phoenix Program[12] with the CORDS system in Vietnam[13] and second through Village Stability Operations in Afghanistan,[14] the U.S. military has retained its industrial-age, attrition-based conventional roots, while facing an undeniably unconventional conflict.[15] So, it remains to be seen how the U.S. military will develop a set of doctrines for strategy and tactics fit for future irregular warfare engagements.

The U.S. military's struggle for fitness does not come from incompetence, but from growing complexity in our conflict and political environments and a long-standing disparity between our model of warfare used to design our military and the actual environments that dominate our military's deployments. In an analysis of 211 years of American military history, the country has been involved in over 300 instances of armed intervention.[16] Yet, this number includes only 11 declared wars, plus some extended campaigns (i.e., Korea and Vietnam). In the decade from 1998–2008, only four of the 30 major conflicts in action were between state militaries.[17]

As further evidence that warfare is not confined to industrialized state-versus-state conflict. Two separate studies[18] make a poignant alert to the value of ungoverned territories, and the complex threats they represent to global security and stability, as well as the inherently social phenomenon that creates the ungoverned space. The conventional paradigm has no model for intervention in truly ungoverned spaces. It is the remoteness, disconnectedness and rustic nature of the actors involved that makes ungoverned spaces–and all low-tech artifacts of irregular warfare–that makes these conventional disadvantages into advantages for irregular threats. This is not because our irregular enemies deliberately choose something other than massive mechanized formations capable of crushing less-formidable mechanized formations through fire and maneuver across the open physical terrain—any insurgent group would be happy to have an armored brigade or two. It is because they inherently possess distinct disadvantages in the material or physical domain (i.e., widespread application of advanced technologies, firepower and mass logistics) and equally strong natural advantages in the social domain. This dramatically impacts their ability to maneuver through the human terrain and bring about consequences tied to their advantages in ways that are invisible to us or beyond effective response by our current methods. In wars amongst the people, our enemies are not able to best our combat forces, so they must negate that force in order to survive; thus they seek to dominate in the information domain.

Arguably, in our technological development over the last 30 years, we have actually prepared for the information war: constructing control-centric technologies and improved firepower, but not improving our understanding. Notions of net-centric warfare have dominated the Pentagon's thinking and have driven us to invest massive intellectual and financial capital in information-technology applications for speeding up our own information flow or empowering the edges of our organizations.[19] No such deliberate effort or investment has been expended by our enemies; the insurgent's use of networks is organic, natural. It is in our self-analytical, high-tech collection and dissemination systems that the environmental information asymmetry defeats us: we are technologically and intellectually equipped to defeat a foe organized, equipped and trained like us. In conflict with dark networks throughout the human terrain we are, in a sense, blinded and trapped by the very systems which we created.

The obvious response, then, may at first seem simpler than it is. We need better technology and better methods. So which comes first? Many distinguished authors have debated as to whether it is technological change or doctrinal change which drives the other[20] and that our lack of control over our technical and doctrinal destiny, as it were, may be indicative of the unpredictable and emergent nature of warfare in the increasingly complex world in which we live.[21] While that debate continues, the strategic and tactical patterns of the wars we face continue to evolve quicker than our ability to understand, organize and intervene appropriately both strategically and tactically. There is always room for better technology, assuming better means more useful to the operator in increasing his awareness, efficiency and capabilities. This thesis takes a hard look at the use of SNA to analyze complex social environments and develop intervention strategies appropriate for warfare against dark networks.

The fundamental concepts for this thesis and network warfare find their roots in complexity theory and social network theory, which introduce new concepts and terms such as nodes and links, embeddedness and centrality, core-periphery, Simmelian ties, trust and reciprocity, structural holes and brokerage. Theories such as complexity theory and others provide the concepts of non-linearity, dynamic and emergent structures, trust, embeddedness, brokerage and the interdependent nature of position and power, culminating in the concept of the key player. System complexity is defined as outputs being disproportional to inputs, the whole not being equal to the sum or the parts, and inconsistencies in the relationship between causes and effects. As applied to network warfare, or netwar,[22] these concepts possess several key aspects which must be understood.[23] Non-linearity and embeddedness are both rooted in the fundamental nature of social networks. The dichotomy between organic (naturally occurring), scale-free and random networks can be described as how complexity and embeddedness arise in social networks.

Randomly distributed networks exhibit normally-distributed levels of connectivity between members across a given network; none are substantially more or less connected that anyone else. Most real-world networks do not exhibit random connectivity; social networks are interconnected according power law distribution. The random network exhibits a normal distribution of relations while the scale-free exhibits a power law distribution of relations where only a few nodes possess a very large number of relations, indicating the presence of key players. One way to describe it is that an actor, because of the scale-free nature of his networked social environment in which he is embedded, can have a disproportionately high number of relations in multiple layers of networks, as in Figure 1.[24] His social network neighbors, again because of the scale-free structure around them, will almost certainly not possess the same number, type or strength of ties with their neighbors. They may not even feel the same way about the first actor as he does about them, and, furthermore, those feelings may change over time; hence, they possess asymmetric and dynamic quantities and qualities of relations.

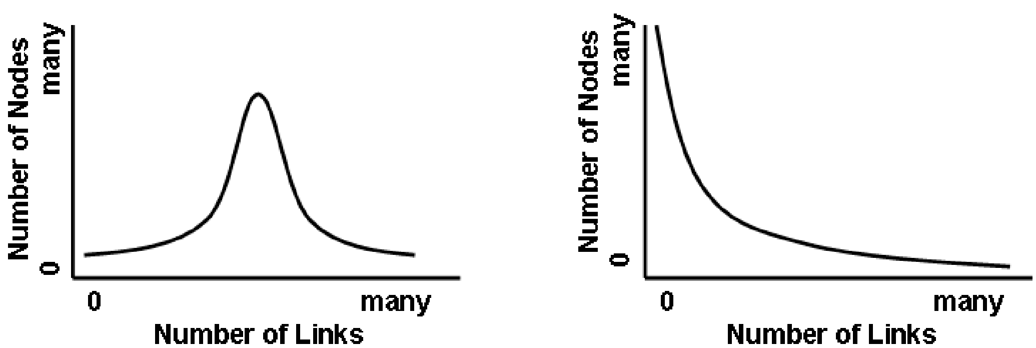

Figure 1. Comparison of random distribution (left) and scale-free distribution (right) of relationships in a social network. From Barabasi and Bonabeau, 2003.

In a manner that follows from uneven relations amongst actors, enters the non-linear nature of complexity. Some actors are better-connected than others in some circumstances, and even the term “better” means different things in different contexts. Varying degrees of connectedness, trust, similarity, knowledge and awareness, access to resources and other factors all contribute depending upon the context under investigation. Some actors will be better positioned in terms of information awareness, and those actors will have power over others because of who they know, who those relations know, and the social distance between them. In practical terms, this means that information will flow unevenly across a social network and that different actors will respond differently, depending upon the information they receive and how they interpret it. Since actors are interdependent on multiple levels, or embedded in multiple networks, there are at least as many ways to reach an actor as there are relations embedded in the social network. The illicit nature of dark networks makes these relations even more tenuous, precious yet vulnerable, and demands secrecy and trust between one another.

For purposes of this thesis, the primary aspect of complexity is that complex systems cannot be understood by simply disaggregating and isolating the parts for scrutiny.[25] In terms of total network analysis, simply taking a network apart and studying the actors or even studying actor dyads (A’s relationship with B) is not going be meaningful. The actors must be understood in their network context. The corollary is that a social network cannot be understood apart from its environmental context.[26] For social networks, this means that a network must be understood by the relations between actors and across the network boundaries within its surrounding social networks. The synergy between the components of the network and the network and its environment must be considered. A second, equally-important factor is the covert nature of dark networks. The critical difference between dark networks and light, or overt, networks, is that the actors, individually and collectively, take actions to conceal relationships, intentions and activities. These characteristics of dark networks exacerbate some inherent SNA planning problems which will be discussed later.[*]

[*] See Chapter 3 for discussion of the three basic planning assumptions for social network analysis.

Embeddedness is a critical aspect of complex systems and, therefore, of netwar.[27] Embeddedness rests upon the foundation that multiple networks or systems in society exist simultaneously and that individual actors and groups are present and act in more than one layer simultaneously.[28] What is significant in this multi-layered existence is that actors accomplish their goals through trusted relations regardless of the layer in which they predominantly exist or interact.[29] Actors tend to give preference to trusted and capable persons and groups who possess information or have known connections to resources rather than to other, unknown and un-trusted actors who may or may not have access to the same information or resources.[30] This holds true for actors within organizations, which contain social networks inside themselves: if the organization's social network reach does not support an actor's goals, then the actor may reach outside of the organization via extra-organizational ties to accomplish those goals.[31] Therein lies a critical vulnerability that may be exploited by another group, such as a counterterrorism or counterinsurgent force and has pertinence to this thesis.

As applied to social networks, the concepts of embeddedness and centrality make a useable theoretical frame in which to identify and discover paths to key players, critical mechanisms, and other exploitable locations or qualities in a network. It is from this position that this thesis departs to describe how combining SNA and the SF Target Analysis process will improve the way in which the military does business in wars amongst the people.

C. STRUCTURE OF THESIS

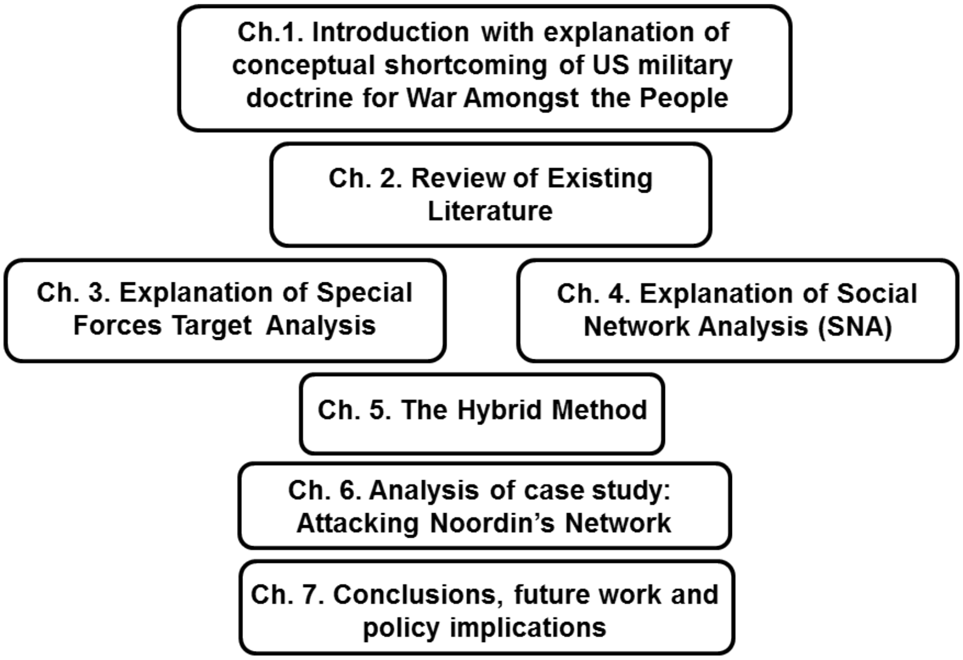

Figure 2. Thesis structure.

This thesis follows the structure depicted in Figure 2. The following chapters begin with a review of existing literature, highlighting a gap between current U.S. military thought and practice and the complexity of wars amongst the people. Chapters III and IV describe the frames and structure of the Special Forces Target Analysis process and Social Network Analysis, respectively, to build the abutments, so to speak, for the bridging concept of the hybrid method, which constitutes Chapter V. Chapter VI is the analytical chapter centered on an open-source dataset of a real-world terrorist network as investigated and published by the International Crisis Group. The last chapter is the conclusions drawn from the application of the hybrid method to the dataset, and continues to recommend future work and possible policy implications for the military, in particular the special operations community, for future forays into wars amongst the people.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW: A SURVEY OF THEORETICAL AND APPLICATION LITERATURE

This literature review surveys the field of relevant research and analysis in military and academic components. The military component in general demonstrates how far military doctrine has come in understanding irregular warfare, but also how it lags behind the state of the art in understanding complexity as applied to systems and social network thinking. These military works cover planning, operations, intelligence, targeting and effects-based operations. The academic component captures the non-military approach to social networks, criminal networks, secret societies (including criminal, insurgent and terror organizations) and what social network analysis, or SNA, has to offer for theoretical and practical support for operationalizing complex analysis and intervention strategies. Included in this review are the works that established or derived the fundamental concepts that support SNA, describe dark networks, a basic level of understanding secret societies and its sociological implications, and military planning in general and as applied to counterinsurgency and counterterrorism. This survey is not intended to be exhaustive, but illustrative of the current state of relevant concepts.

A. AMERICAN MILITARY LITERATURE AND DOCTRINAL PUBLICATIONS

The military literature component is drawn primarily from the Army's field manuals, including the Army's doctrine and implementation publications; the joint, or inter-service, intelligence and operations publications; and Special Operations publications.[32] All of these documents have been published since 2001.[33] The academic component comes mainly from the field of social network analysis, but also from the fields of social movement theory, econometrics, secret societies and organized crime. The documents for this component go back to 1908.

The root assumptions behind the Special Operations Targeting Process (SOTP), specifically the Special Forces Target Analysis process, hereafter referred to as "SF target analysis," and SNA stem from a common frame which provides a critical theoretical bridge between the two processes. The SF Target Analysis process and SNA see the world as a system of systems or a network of networks, respectively, which are compatible views of the world. Traditionally, SF Target Analysis views the levels of interconnectedness between systems within systems mainly as hierarchical and contained within the larger system–vertical interdependence –but not necessarily as interdependent horizontally across peer systems within the environment except at the highest level.[34] For the purposes of this thesis, however, a useful comparison can be made using the concept of vertical *and horizontal* interconnectedness of the conflict environment used in center of gravity analysis. With one critical exception, most of the joint publications describe *de fact*o embeddedness, but never fully articulate the resulting dynamics at work other than stating that actors, influences and intervention effects are interconnected.[35]

The inherent social network characteristic known as embeddedness means that networks exist within and amongst other networks, such that the networks and the transactions within and between them are inseparable from one another.[36] While not exactly identical, the fact that both of these analytical processes have a principal notion of interconnectedness and interdependency means that most, if not all, other aspects of the processes could have strong levels of equality or, at least, should not be completely foreign to each other.

However, it is not in this similarity that SNA offers advantage to the user as the similarity is just a bridge connecting the two processes' base concepts. It is in the differences between the two that SNA offers its advantages. The difference is rooted in the framing and application of complexity in the approaches. As such, the disadvantage of the traditional application of systems thinking is the linearity of the methods described in various publications. That is, the analytical and intervention planning methods were not formed around complexity thinking. The advantages to SNA are embodied by complexity thinking as detailed earlier in this chapter. This is manifest in the ability of SNA to detect and evaluate patterns of relationships and attributes of a network *as a whole*, providing insight into the structure and distribution of power (or, access and placement) across that network. These patterns come from the measurements of centrality and other measurements available only through SNA. Despite this stark difference, traces of common theoretical lineage are not found only between SNA and the SOTP. In fact, there is a closer fit as we elevate our level of analysis to the strategic level, but it still falls short of fully implementing network thinking into our modern targeting methodology.

The concept of identifying centers of gravity, or COGs, as portrayed in JP 3-0 and JP 5–0[37] and to a certain extent in FM 3-05,[38] essentially describes embeddedness of multiple actors and influences at the strategic level. However, the authors of JP 3-0 and JP 5-0 only make use of link analysis which is dyadic in its level of analysis (A is connected to B and B is connected to C, etc.) and does not lend itself to discovering what the entire network looks like or how it is constructed, let alone measuring power distribution across the network. As a second flaw in the joint publications, upon seeking a framework for development of a consistent implementation strategy, the military authors fall back into a linear paradigm with the Lines of Operation method of implementation. JP 3-60 Joint Targeting does initially portray targets as a system of component systems. To its credit, it does not utilize the Lines of Operation implementation methodology but, rather, it uses an even more linear discrete cyclical process of one cycle per target without regard for fractal effects of the success or failure of that one cycle. However, to its discredit, JP 3-60 does not allow for making cycles contingent upon the effects gained (or lost) from targeting cycle to targeting cycle. In most military models of intelligence and operational cycles, they are treated as discrete events, not modified or otherwise adapted from one iteration to the next. Nor does it allow for anything inching closer to acknowledging potential target complexity: horizontal interdependence across systems, sub-systems and components. Overall, measures of effectiveness do not create an analytical framework capable of detecting or measuring fractal effects of targeting cycles. The authors of JP 3-0 and JP 5-0 and, most of all, JP 3-60 begin down the trail of complexity, systems and embeddedness, but then jump back onto the track of traditional, linear intervention systems approaches when proscribing interventions and assessing changes. Thus, the U.S. military institutionally stops itself short of implementing complexity principles or a systems view in its operational- and tactical-level analysis and operations and limits its analytical processes to static link analysis, leaving the operational and tactical levels without a useful, modern planning framework at all.

Within the special operations publications, an interesting dichotomy arises. There is a curious gap is between the rather meticulous deconstructionist approach of the SF Target Analysis process, known by the acronym CARVER, and the fact that the rest of the publications concerning Unconventional Warfare, Operational Preparation of the Environment, and Foreign Internal Defense make no detailed explanation of the advantages of understanding networked insurgent groups or other social systems. All three exclusively concerned with irregular conflict. A comprehensive analysis of the etymology of the SOTP and CARVER methodologies reveals a disparity between the Army SOF doctrine as written in FM 3-05 and that as written in FM 3-05.20 Special Forces Intelligence Operations and the joint SOF doctrine embodied in JP 3-05.2. The disparity at issue arises in the authors' complete lack of conceptualization of systems thinking in military operations. The Army SOF manual has a much more comprehensive complexity-minded approach to assessing and evaluating targets not merely as technical systems to be reduced to their parts, but as a framework for disaggregating a complex socio-political structure of a conflict while maintaining the interdependent nature of the environment. The Army SOF manual draws this particular lineage from the previously-discussed strategic joint manuals JP 3-0[39] and JP 5–0[40] but with some detracting issues. Another strategic variation exists in JP 3-60 Joint Targeting, but suffers from the same root issues as the former manuals: a bias toward linear, kinetic intervention. As such, FM 3-05, JP 3-0, JP 3-60 and JP 5-0 incorporate a broader application of complexity concepts than does the Joint Special Operations publication JP 3-05.2.

An important inconsistency arises in these publications, but most vividly within JP 3-60. Its bias toward kinetic targeting undoes its progressive thinking in analysis by linearizing the intervention approach; that is, it would have the U.S. military attack a target as if the target were a unitary actor, rather than a system of systems with vulnerabilities distributed throughout the environment as the manual states. In this way, targeting practitioners using this doctrine, while they may have properly framed the environment, are limited from many intervention options and maximizing and measuring the effects of those intervention methods as is so strongly stated by these publications. It is this author's belief that this is because the assessment process is not supported by a methodology capable of framing or measuring such complex environments. And with no way to thoroughly measure the initial conditions, how is measurement of changes due to intervention strategies possible? It is not, except by anecdote or perhaps keen intuition of the aggregate. In sum, readers of JP 3-0, JP 3-60, JP 5-0 and FM 3-05 would come away with an understanding of strategic-level interdependence (mostly as it pertains to center of gravity analysis; see Figure 3) and those of JP 3-05.2 and FM 3-05.20 only would be relatively unprepared for the theoretical leap from link analysis to SNA but would still have a basic understanding of interconnectedness between layers of systems.

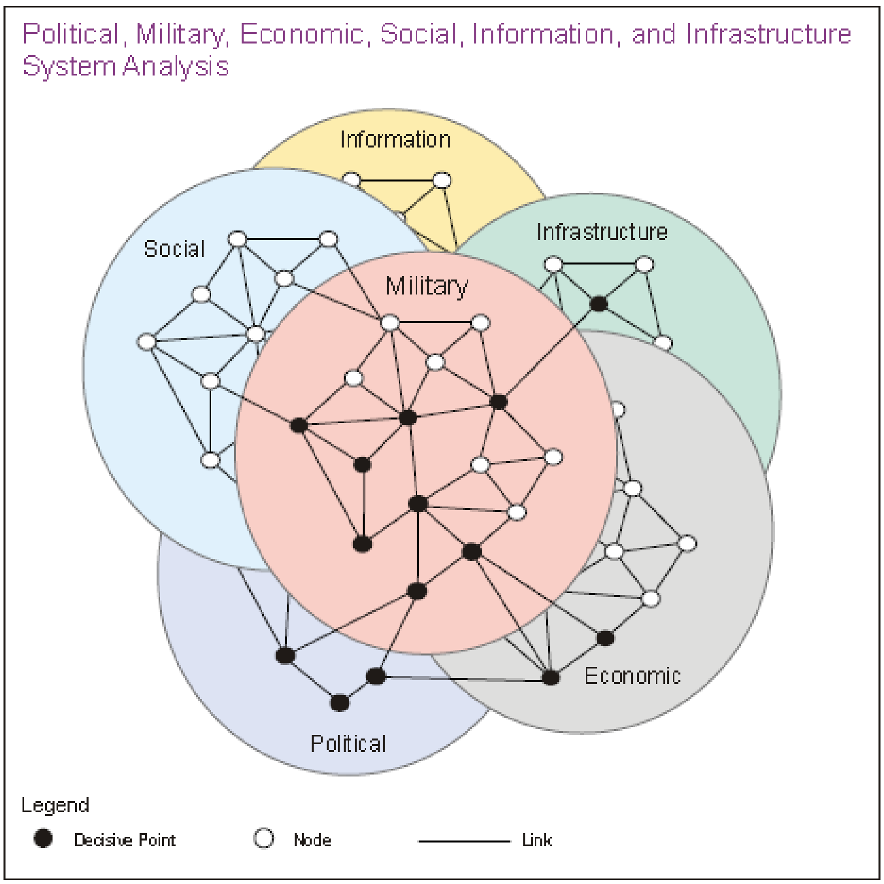

Figure 3. Joint doctrinal graphic from that uses the PMESII framework to demonstrate the interconnectedness—embeddedness—of the operational environment and alluding to a systems method of analysis. From JP 5-0 Joint Operation Planning, 2011.

In a significant departure from the trend described above, two of the latest Army manuals, FM 3-05.201 Special Forces Unconventional Warfare, FM 3-24 Counterinsurgency,[41] TRADOC Pamphlet 525-5-500,[42] and a Joint Warfighting Center handbook[43] make substantially more use of complexity or systems thinking in their descriptions of the conflict environment and interdependence of actors contained within. However, while both of the first two manuals spend a good amount of time telling the reader to perceive the environment as complex, neither provides a framework for analysis of the social and political aspects of the environment or conflict. This lack of analytical framework leaves the military wanting for a structure in which to couch any intervention strategies, let alone a system of metrics to assist in constructing a strategy or being able to determine the outcomes of intervention. In this regard, both of these manuals cease injecting complexity into analysis and operations at the same point as the joint targeting publication (JP 3-60), though they continue stressing complexity of intervention in irregular warfare environments.

The counterinsurgency manual possesses an appendix on social network analysis, but it erroneously portrays centrality measurements as something that tactical units can conduct as they are currently structured and trained. FM 3-24 also implies that the information gleaned from SNA can be boiled down to over-simplified matrix-style charts for distribution to subordinate units. While it looks appealing in its simplicity, the methods disintegrate when dealing with larger datasets in the real world. The use of SNA software packages is mentioned nowhere, so unit commanders and officers attempting to direct their soldiers and analysts to determine high value individuals are left without a paddle, so to speak, as resort to intuition. Overall, while it does not do the military a great deal of help in framing and understanding complex interdependence, the current counterinsurgency manual goes the furthest in implementing SNA for understanding the environment as well as identifying key players as contained within.

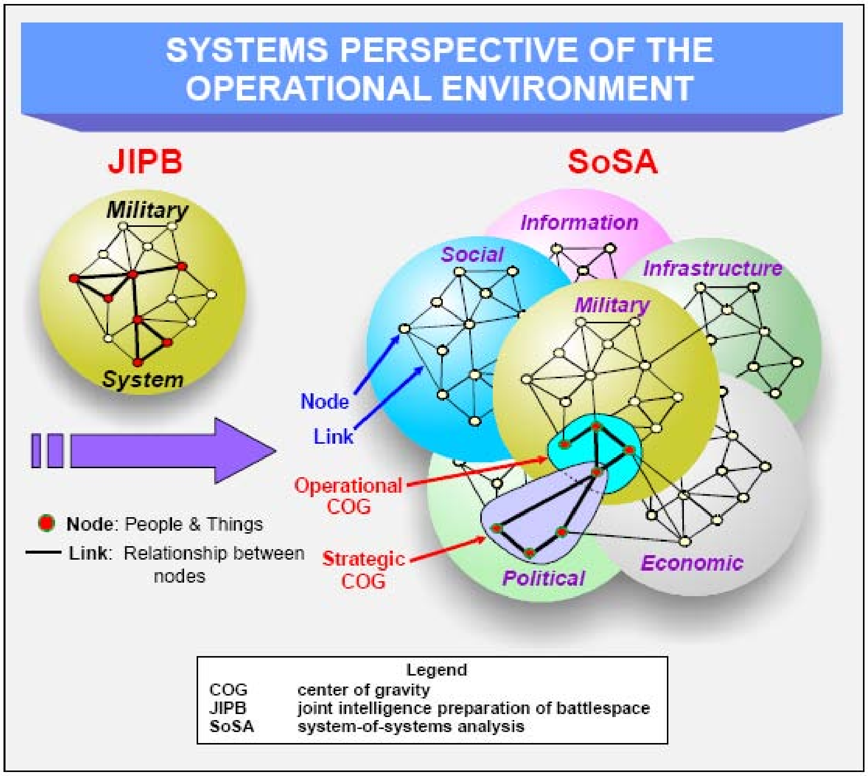

Figure 4. A first military description of a strategic-level system of systems perspective. From JWC's Effects-based Approach to Joint Operations handbook.[44]

However, the Joint Warfighting Center's *Commander's Handbook for Effects-Based Approach to Joint Operations* is a light in the dark, compared to the rest of the military literature in its attempt at instilling a systems perspective in military planning and operations. This document went very far in its analysis and application of systems thought as it viewed the world of warfare as a system of systems (Figure 4). It did not stop there, as it also goes on to describe the depth and importance of key nodes and some description of embeddedness, though it did not refer to it as such.[45] Unfortunately, in one of its last years in operation, GEN James Mattis, USMC, dismantled U.S. Joint Forces Command's EBO school of thought.[46] Ironically, Defense Secretary Robert Gates soon afterward announced the command would be shut down.[47]

The next problem identified is that of assessment and evaluation of the environment and changes due to intervention and other factors. Said another way, how to measure initial conditions and changes in the conflict environment to indicate patterns, trends and trajectories of the myriad of factors in modern conflict environments. While several military publications make mention of the need for appropriate metrics and may or may not give boundaries to the usable conceptual space for those metrics, none go as far as TRADOC Pamphlet 525-5-500,[48] JP 3-60,[49] or the Joint Warfighting Center's Commander's Handbook for Effects-Based Approach to Joint Operations. Yet, even these publications do not offer a systemic framework for measuring a consistent type of information throughout all levels of analysis and to every conflict and across the operational spectrum: characteristics of the relationships between actors and of relationships across networks embedded within the conflict environment before, during and after intervention. The concept is applied at the strategic and campaign level and without word of its applicability at lower levels or how to implement it. In sociological terms, there is ample space in these last two publications for proposing SNA as an effective method for understanding the environment, but none whatsoever for using it to assist prescribing an intervention strategy or guiding the future analysis of changes in the environment post-intervention. They both, however, open the reader's mind to understanding a fractal spread of effects across an area of military operations, which is certainly a step in the right direction.

This brief review of joint military, U.S. Army conventional and special operations doctrine reveals inconsistent and incomplete use of complexity and systems thinking to frame and describe analysis and planning in complex environments, though all publications make mention of the increasingly complex nature of the operating environment. For a brief overview assessment of the applicable publications, see Table 1. Next, a review of civilian academic SNA literature is necessary to determine what this field offers to bolster the military's analytical and targeting processes in modern conflict.

Publication	Uses complexity or systems thinking... In assessment and evaluation	In developing an intervention strategy
FM 3-05 Army Special Operations Forces (U)	some	no
FM 3-05.20 Special Forces Operations (C)	little	little
FM 3-05.201 Special Forces Unconventional Warfare (S/NF)	some	some
FM 3-05.232 Special Forces Intelligence Operations (U)	little	no
FM 5-0 Operations (U)	no	no
FM 5-0.1 Operations Process (U)	no	no
FM 3-24 Counterinsurgency (U)	some	little
JP 2-01.1 Joint TTPs* for Intelligence Support to Targeting (U)	little	no
JP 2-01.3 Joint TTPs* for Intelligence Preparation of the Battlefield (U)	no	no
JP 3-0 Joint Operations (U)	some	no
JP 3-05 Doctrine for Joint Special Operations (U)	little	no
JP 3-05.2 Joint TTPs* for Special Operations Targeting and Mission Planning (U)	little	no
JP 3-60 Joint Targeting (U)	some	no
JP 5-0 Joint Operation Planning (U)	some	no
TC 31-16 Special Forces Operational Preparation of the Environment (S/NF)	little	no
TRADOC Pamphlet 525-5-500 Commander's Appreciation and Campaign Design (U)	much	some
Irregular Warfare Joint Operating Concept (U)	some	little
JWC's Commander's Handbook for an Effects-Based Approach to Joint Operations (U)	much	some

Table 1. An assessment of joint military, Army and Special Operations Forces publications' use of complexity and systems thinking to assist in analysis and strategy development.

B. CIVILIAN ACADEMIC LITERATURE.

For the application of SNA to social science problems—such as dark networks—there has been an explosion of literature describing the emergence of complexity and interdependence of actors and their activities in society. Works from Barabasi,[50] Holland,[51] Lewin,[52] and Waldrop[53] established a pattern of literature looking at the aspects of complexity and interconnectedness in the modern world—specifically modern societies interconnected by the Internet and other artifacts of the information age. It is interesting to note that many of the authors did not have sociology backgrounds. Rather, they were physicists, biologists, businessmen and economists. As they applied this complexity thinking to larger social and physical phenomena, a top-down-oriented school of thought began to form. This grew to include international and military affairs.

The Pentagon's Command and Control Research Program (CCRP) created an environment where James Moffat's,[54] Edward Smith's[55] and Albert, Garstka and Stein's[56] works came to encompass the leading-edge thought on network-centric warfare in an effort to morph American military doctrine to pattern itself after natural complex adaptive systems which demonstrate characteristics that allow those systems to adjust to threats and changes in the local environment in the name of survival. Despite the research and prescriptions offered by these and other authors spurred by Defense Secretary Rumsfeld's desire for a leaner, more high-tech, "information-age"[57] force, this desired outcome has yet to be realized.

Prior to Secretary Rumsfeld's time in office under President George W. Bush, however, John Arquilla and David Ronfeldt had envisioned future conflicts not merely involving high-tech networks of armored vehicles and future-soldiers, but a social version of cyberwar, meaning decentralized power structures adapting to and taking advantage of pre-existing systems and influences in the environment: "These protagonists are likely to consist of dispersed organizations, small groups, and individuals who communicate, coordinate and conduct their campaigns in an interdependent manner, often without a precise central command."[58] Much more recently, Brafman and Beckstrom illustrated the social reality of these trends in their analysis of both legitimate and extralegal leaderless organizations.[59] Their work indicated what had been brewing in the sociology world for some time: that social adaptation will breed complexity.

While the top-down thought approach described above is relatively young, social scientists had been looking at all things interconnected from the bottom-up for decades. For example, a seminal paper used in this research by Mark Granovetter entitled "The Strength of Weak Ties" was published in 1973.[60] However, the basis for SNA application does not originate solely in the quantitative sociology and SNA literature.

The studies of history, international terrorism policy, criminology social and revolutionary movements, and even healthcare offer a broad array of examples of theoretical and practical aspects of systems thinking in successful, unsuccessful and undetermined conflict outcomes from various types of belligerents' perspectives. I draw upon all these sectors of SNA-related literature for my thesis. Spanning decades, fundamental SNA publications by Wasserman and Faust,[61] Simmel,[62] Burt,[63] Freeman,[64] Hanneman and Riddle,[65] DeNooy et al., Borgatti,[66] and Scott[67] are the basis for much of the present day SNA procedures and research, including this work. More than a century ago, Simmel applied the fundamental concepts to the phenomenon of secret societies, noting fundamental differences that secrecy demands. Wasserman and Faust, Hanneman and Riddle, and Freeman compiled the basic concepts and processes behind SNA. Scott's handbook brings the Burt's analysis of economic competition changed the way in which we look at competition between people and in the commercial marketplace. Borgatti and Freeman created UCINET, a landmark piece of SNA software originally developed in the 1980s.[68] DeNooy et al., created a SNA program called Pajek, which has some operational advantages over UCINET. A next step in approaching the analysis of networked organizations problem is covered by Kilduff and Tsai[69] and Monge and Contractor,[70] expanding on the previous authors' work and approached SNA application from a multi-disciplinary perspective. Krebs[71] analyzed the 9/11 terrorists' connections using SNA, bringing it to higher level of popular attention. For purposes of this thesis, all of the measures of centrality and indicators of characteristics of social networks, as well as multi-disciplinary applications, are contained in these authors' collective work.

Other pieces that strongly influenced this thesis are immediately concerned with a subset of social networks called dark networks. Originally considered by Georg Simmel in his work on secret societies,[72] the idea of analyzing intentionally-concealed social constructs grew as others (Hazelrigg[73] and Erickson,[74] for example) re-examined his ideas and combined them with developments in the field. The idea of dark or covert networks—including insurgent and criminal organizations—has been of interest for some time and inspired authors like Sparrow,[75] Klerks,[76] and Reed.[77] Sparrow and Klerks looked at criminal organizations and Reed analyzed the insurgency in Iraq as a SNA problem. In fact, Sparrow's basic assumptions for analysis of dark networks are critical and hint of a quantitative science intertwined with analytical art. One of the landmark works on the subject came from industry, by Baker and Faulkner, extending the idea that dark networks can arise from light, or visible, inter- and intra-organizational relations.[78] Interest in the subject exploded with the advent of international terrorism and, in particular, the attacks of September 11, 2001. The idea of dark networks has since been elaborated by Raab and Milward,[79] who coined the term and approached the issue from a policy problem perspective; and Rodrigues,[80] who proposed that the superb security and secrecy of the Atocha, Spain train bombers (the "3–11" attacks in 2004) was in the weakness of the ties between them; his analysis builds on another aspect of Granovetter's "Strength of Weak Ties" in that those distant relations make them difficult to discover and disrupt. Valdis Krebs gave the 9–11 hijackers a thorough analysis using his In-flow software.[81] Finally, Stuart Koschade, in his analysis of Jemaah Islamiyah,[82] demonstrated that SNA of covert groups is possible, albeit postmortem, and can bring about useful information about such groups' structure and internal dynamics. This analysis of JI as a dark network dove-tails neatly into this thesis, as JI played a significant role in Noordin Mohammed Top's network, which is the subject of analysis in Chapter 6.

Agent-based modeling computer modeling has been used to study dark networks, both from a pure research perspective[83] as well as a test bed for intervention techniques.[84] Here, Kathleen Carley, with Maksim Tsvetovat and others, has been relatively prolific in publishing her findings using her PCANSS dynamic network modeling schema.[85] Carley has not been the only one to advance intervention strategies. Nagaraja and Anderson[86] proposed a limited but interesting set of naïve offensive and defensive strategies in virtual simulations, which give insight into possible fundamental strategies to be adjusted for real-world application. Some of the ideas behind Carley's and others' attention to network dynamics and intervention strategies include understanding the impact of an actor's position in their network, partly as measured by their centrality.

Enter the concept of the key player, who derives his importance from their position for either diffusing information into and across a network, or vis-à-vis their removal and the subsequent fracturing effects upon that network. A key player's power is derived in part from his centrality. This concept owes much to the work of Stephen Borgatti[87] who, among a great many other aspects, looked at specifically identifying key players in a networked environment. In an older article, Phillip Bonacich[88] has developed a method to analyze overlapping memberships, which is important for accounting for actor embeddedness and the idea of exploiting multiple pathways to reach a targeted actor. He also explored the eigenvector centrality[89] which gives us centrality measurements of actors by the quantity of their network neighbors' contacts—the quintessential "knowing people who know people." Additional measures of centrality attempting to better refine the key player problem of network intervention targeting, are described in pieces by Ballester, Calvo-Armengol and Zenou.[90]

As a military practitioners go, one of the first to capitalize on the work being done at Naval Postgraduate School, John Dodson drew a linkage between dark networks, small world phenomena, and "nexus" topography under the concept of man-hunting.[91] Also, Brian Reed authored an article on SNA and Insurgency[92] and co-authored the SNA appendix in the Army and Marine Corps' new counterinsurgency manual; and Jonathan Hammill focused on simultaneous analysis of layers of networks in intervening against near-term terrorist attacks.[93] As testament to the new way of thinking as applied once in Iraq, the military's capture of Saddam Hussein has been documented as a success of implementing aspects of SNA.[94] For attacks on distributed networks, an important branch of investigation is into recovery from attack. Here, again, Carley used her dynamic modeling simulations to determine that cells within dark networks are able to overcome simple attacks (removal of single or few key nodes) by reconnecting via latent relations outside the clique or cell.[95]

Specific to the current conflicts in Iraq and Afghanistan, the Improvised Explosive Device, or IED, as a social phenomenon was the subject of study by Montgomery McFate[96] and the term "viral" first appeared in the military-oriented literature in a work by Scott Swanson[97] that described a following-the-links approach to targeting of IED cell members and supply chains. Another important aspect of maintaining a dark network is contained within the struggle between efficiency and security, which was analyzed by Bienenstock and Bonacich.[98,99] A last note on new directions for the study of dark networks and their capabilities comes from work by Simson Garfinkel,[100] Marc Sageman,[101] Brafman and Beckstrom,[102] and Amoss,[103] who was an army officer concerned about American military and governmental continuity after a Soviet invasion in the 1960s. He was cited by the American white-supremacist and secessionist Louis Beam, who looked at leaderless networks and their ability to overcome traditional direct-attack intervention methods as a form of resistance to federal invasion into citizens' rights. Overall, these authors analyzed and appreciated the phenomenon of so-called “leaderless” networks, or those whose deliberate, decentralized structures precludes disruption by centrality-based node removal.

From this survey of the relevant military and academic literature and their associated theories, it is evident that the time is right for military thought and doctrine to encompass complexity in conflict environment analysis and development of intervention strategies. While this thesis deals with a fairly specific set of measurements and processes, the larger field of social network analysis has much more to offer the military and, more specifically, Special Operations, which was created for ambiguous and complex conflict environments. The effectiveness of the analysis and intervention strategies outlined in the following chapters is only a small set of examples of what is possible with SNA.

III INTRODUCTION TO THE SPECIAL OPERATIONS TARGETING PROCESS

The Special Operations Targeting Process, or SOTP, is intended to support American military strategy provided by a strategic-level command through multiple echelons and a coherent series of tactical actions intended to have effects greater than the sum of the actions themselves. This chapter describes the three layers—or echelons—of targeting, the way the SOTP supports conventional targeting, and target evaluation, selection and prioritization methods.[*] By the end of this chapter, the reader should understand the SOTP process and the CARVER[†] method of target evaluation.

In pursuing American foreign or defense policy at the strategic level, problems or problem sets can be framed according to geographic regions, which supports the Defense Department's geographic orientation of the Geographic Combatant Commands, or GCCs.[104] If a defense problem is defined as global or specific to an assigned function of another command, such as international terrorism conducted by al-Qaeda and its associated networks and ideology,[105] then another Unified Command with global or appropriate functional responsibilities, such as USSOCOM,[106] takes overall responsibility for properly framing the problem and deriving the ends, ways and means to resolve the national security problem and its contributing causes.[107] In either case, a strategic-level command will frame defense problems and threats as strategic problems.

At the strategic level, all wartime and non-wartime campaigns are top-down directed by national security decisions through the Pentagon and include a special operations component. Employment of SOF in a non-wartime environment has always been a tricky issue,[108] but this is what most special operators were accustomed to prior to 9/11 and what was taught at the Special Warfare Center at Fort Bragg, NC.[109] Once a Congressional or Executive Branch directive and authority was established for given

[*] Specific tactics, techniques and procedures of reconnaissance and surveillance, asset recruitment, assaulting an objective area, and exploitation of captured human and technical targets will not be discussed. This chapter provides an overview of analytical and planning processes leading up to and following an actual assault or other operation.

[†] CARVER is a military targeting mnemonic meaning Criticality, Accessibility, Recuperability, Effect, and Recognizability, and is explained in detail later in this chapter.

security issue, the Geographic Combatant Command's planning and targeting began, with SOF involvement at the TSOC level and then directs further SOF involvement descending to the tactical level. Figure 5 depicts the strategic to tactical levels of war and corresponding organizations pertinent to this thesis.

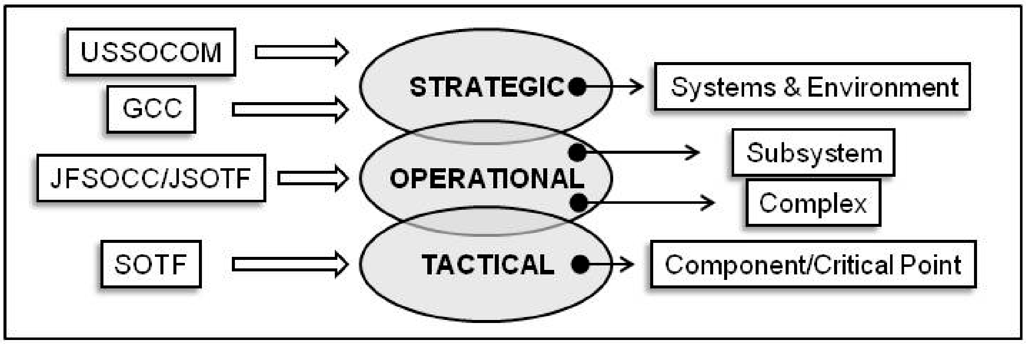

Figure 5. Echelons of the chain of command, the associated the levels of war and levels of target analysis.[110]

SOF targeting has traditionally been a Theater Special Operations Command, or TSOC, function subordinate to the GCC and, when applicable, supporting a Joint Force Command's (JFC) targeting process. Intelligence collection and analysis occurs at multiple layers beneath those echelons, dominated by human intelligence, or HUMINT, and signals intelligence, or SIGINT, and each of the task forces may conduct their own intelligence collection and operations, but traditional operations were predominantly directed by a higher headquarters such as a GCC or JFC. SOF's own operational and tactical target development was limited to local reconnaissance preceding a raid. Thus, in the traditional instance, the SOTP occurs by direction of the supported GCC or JFC as a product of its own targeting process.

The other instance is when a JFC that is operating within a GCC's Area of Responsibility requests support from the GCC, or from the assigned Joint Force Special Operations Component Command, or JFSOCC, in the form of a target or target set[*] which meet the criteria for SOF employment. In the military doctrine literature, this is the

[*] A target set is a group of targets related by geographic proximity, patterns of membership, communications or other associations.

bottom-up fashion—obviously as viewed from the GCC's perspective. Neither of these models, however, addresses the internal operating environment within SOF, particularly within a Joint Special Operations Task Force (JSOTF), or a subordinate Special Operations Task Force (SOTF), where bottom-up targeting from the tactical level is the norm.

Since 9/11, targeting has also become a USSOCOM function as a product of the GWOT synchronizing task as directed by the Secretary of Defense.[111] Today, there are instances where target analysis and subsequent operations of this kind are conducted in a bifurcated manner, with a GCC *and* USSOCOM formulating strategies and directing supporting operations to the Joint Force Special Operations Component Command (JFSOCC). Additionally, during the wars in Iraq (2003–2011) and Afghanistan (2001-?) and other places, SOF played a leading role in targeting insurgent leadership and underground infrastructure.[112] Meanwhile, special operations task forces constantly collect information to feed the intelligence cycle, conduct intelligence analysis of their own, and conduct derived or directed missions in support of a JFC or TSOC strategy and intent.

The GCC identifies the strategic-level systems of interest, such as a network of relations between physical geography, socio-cultural groups, political entities, technology, religions and external relations using the PMESII framework.[*] The GCC then frames the intervention strategy to inform the ends, ways and means planning methodology along the lines of that framework. Thus, the strategic level of analysis is established. Then the resource requirements and lower levels of analysis can be defined and bounded. The military's actions at the operational and tactical levels of war follow directly from the strategic analysis that includes defining the strategic goals, limitations and boundaries of action and the mission and intent[†] of the GCC for a subordinate Joint Force Command, or JFC. That subordinate command then operationalizes the higher

---

[*] See Figures 3 and 4 in Chapter II, PMESII is a framework for describing the interrelated elements of a society in conflict: Political, Military, Economic, Security, Information and Intelligence.

[†] The commander's intent is an explicit statement of the purpose of the operation, the desired end state and definitions of acceptable and unacceptable levels of types of risk.

headquarters' strategic goals, mission and commander's intent for action. It then directs tactical units to fulfill mission objectives[113]

The SOTP delineates types of targets according to the effects of intervention against the enemy. Strategic targets are those which successful intervention would contribute to the GCC's strategic objectives. Successful intervention against operational targets means that the supported JFC commander's operational plans are positively influenced. Tactical targets normally do not meet SOF mission criteria[114] (particularly in support of a conventional force) but may become important in developing the skills of a host nation's military or police forces against a common enemy.[115]

The SOTP, which is a SOF-specific subset of the conventional military Joint Targeting Process, uses a fusion of operations and intelligence functions to efficiently and holistically attack a system of systems from a position of widespread understanding of the structure of and relations between potential military targets. Such potential targets within a foreign country come in two categories: physical, such as communications systems, transportation infrastructure, or electrical power grid networks; and human, such as the social networks of terrorists, insurgents, political parties, industries, or tribes.

The SOTP frames the overall target systems as interlocking sub-systems, complexes and components which are also intended as levels of analysis. These levels of analysis can be framed as parallel to levels of war; that is, the strategic, operational and tactical levels. Echelons of the military chain of command also correspond to the levels of war, and have specific responsibilities for the different levels of target analysis in support of an overall theater strategic campaign. The theory behind pairing the levels of

analysis of the target system with the levels of war is that the planning goals and limitations at each echelon vary enough that the levels of analysis appropriate to understand and achieve those goals must also vary.

While this model of the levels of war exists to delineate levels of analysis and bureaucratic responsibilities, this thesis deals with the technical analytical and operational aspects and not the administrative or logistical aspects contained within each level. It is important to understand the separation of responsibilities per each echelon to see how it compares to the networked threats we face, as well as how the SOF targeting process is different from the conventional process. See Figure BBB for one example of a theater SOF chain of command from USSOCOM to a SOTF.

The U.S. military defines the levels of war as strategic, operational and tactical:

Strategic: "In the context of military operations, strategy develops an idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives."

Operational: "The operational level links the tactical employment of forces to national and military strategic objectives."

Tactical: "Tactics is the employment and ordered arrangement of forces in relation to each other. Joint doctrine focuses this term on planning and executing battles, engagements, and activities at the tactical level to achieve military objectives assigned to tactical units or task forces."[116]

The strategic level of war is where the national military strategies are converted into theater or country-specific campaign plans. The ends, ways and means of resolving a strategic problem is combined with strategic capabilities and resource constraints, and evaluated in terms of risk to provide the design space for a strategy. For special operations, USSOCOM and the GCCs develop global and regional strategic plans, which direct TSOCs and JFCs to plan operations (including tasking subordinate units with missions supporting the operation). Those tactical units conduct their assigned missions and provide intelligence feedback into the operational and strategic echelons. These JFCs and TSOCs direct subordinate SOF elements in accordance with the task organization as outlined in Figure 6.

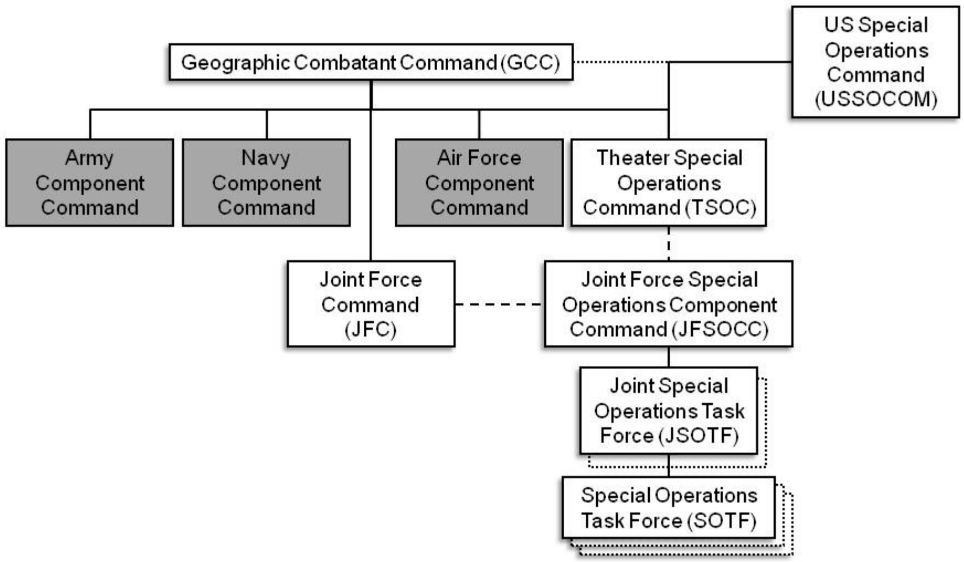

Figure 6. An example of a theater SOF chain of command from USSOCOM to SOTF. The Army, Navy and Air Force components are not part of the special operations chain. The solid lines represent direct operational control of lower echelons; the dashed lines represent optional command relationships dependent upon mission requirements as directed by the GCC.

Each level of war is dependent upon the others, or else a major portion of the problem goes ignored, misunderstood, or unrealized. And every strategy must be operationalized, which requires operational-level plans and enabling instruments, to affect tactical actions, thereby achieving success. As part of the planning process, all echelons of SOF are free to initiate their own targeting beginning with the strategic framework as detailed from the GCC, TSOC or USSOCOM. The conventional military does not do this; higher headquarters designates specific targets for action by tactical units. However, the freedom to develop and engage targets at all levels is crucial for SOF success in that it creates faster responses to changes or new information and rapid exploitation of enemy weaknesses and vulnerabilities. This process is intelligence-intensive and can require outside expertise in describing and evaluating technical or unusually complex targets.

The strategic level of war is where the national military strategies are converted into theater or country-specific campaign plans. The ends, ways and means of resolving a strategic problem is combined with strategic capabilities and resource constraints, and evaluated in terms of risk to provide the design space for a strategy. For special operations, USSOCOM and the GCCs develop global and regional strategic plans, which direct TSOCs and JFCs to plan operations (including tasking subordinate units with missions supporting the operation). Those tactical units conduct their assigned missions and provide intelligence feedback into the operational and strategic echelons.

SOF targets are intended to be operational or strategic in value, so the corresponding value of targets must be understood at the tactical level, where the action takes place. If a target that a tactical SOF unit is supposed to action does not have value at the strategic levels—or least at the operational level—then it is likely that the target will be passed to the conventional military or, in peacetime, remain un-actioned. In this way, the level of analysis at each of the levels of war has deterministic effects upon implementation plans and actions. Figure 7 depicts the tactical organization of SOF—the SOTF, or Special Operations Task Force.

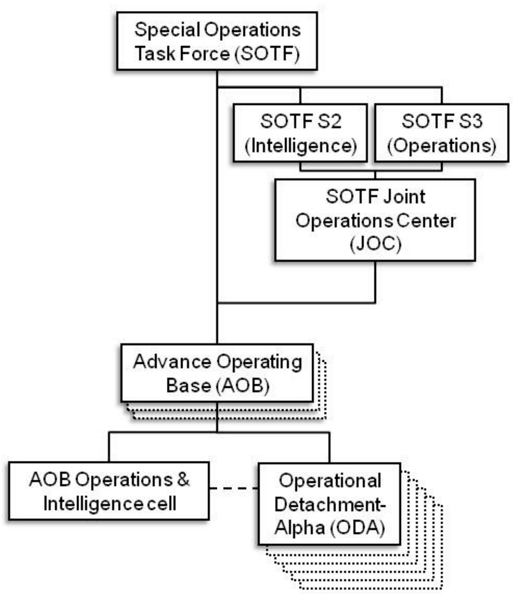

Figure 7. An example of SF operations and intelligence organization within a SOTF.[117]

For the military, the operational level is located between the strategic and tactical levels of war and is intended to be the domain in which commands and staffs design plans for implementation of the strategic direction and intent issued by the GCC. Generally, it is at this level that the JSOTF interfaces with the TSOC to receive direction and guidance and translate that into direction and resources for the SOTFs and other subordinate SOF elements. Simultaneously, the JSOTF develops its own supporting framework to further enable it to meet the strategic-level requirements. In conducting its analysis, the JSOTF functions are supposed to bridge the information and resource requirements of the long-range strategic intent to the daily tactical activities. Its analysis informs the subordinate tactical SOTF headquarters of mission and information requirements.

The tactical level of operations is where operators and practitioners employ their skills and interface with the environment, both requiring and creating space for strategic impact by tactical action. This is one of the primary areas where the differences between special operations and conventional forces become apparent: where conventional operations seek to establish standardized methods of reducing uncertainty and problem solving, special operations forces do not necessarily have that luxury. Because their operational units are so small, SOF must be intimately familiar with the local environment. In social network terms, they must know who the key players are the and relationships between them for any given problem, which places enormous demands upon their regional orientation, linguistic capabilities, and cultural awareness. Oftentimes, the first lesson is to accept that you are a guest in an alien culture, and you must remain perceived as respecting those norms and abiding by those constraints, whatever they may be. The conventional military paradigm for operations and tactics is routinized actions with immediate feedback, while the SOF paradigm is exactly the opposite.[118]

SOF culture, structure and communications are focused downward, with an expectation of intense collaboration between tactical units. SOF approach each problem as unique and requiring a high level of awareness and acuity with a strong emphasis on understanding, inclusivity, creativity, legitimacy in the eyes of key stakeholders, and an eye toward long-term consequences of actions and desired outcomes.[119] See Figure 8 for the tactical organization of theater SOF. These concepts form the basis for the special operations targeting at all levels of war.

A. THE SPECIAL OPERATIONS TARGETING PROCESS

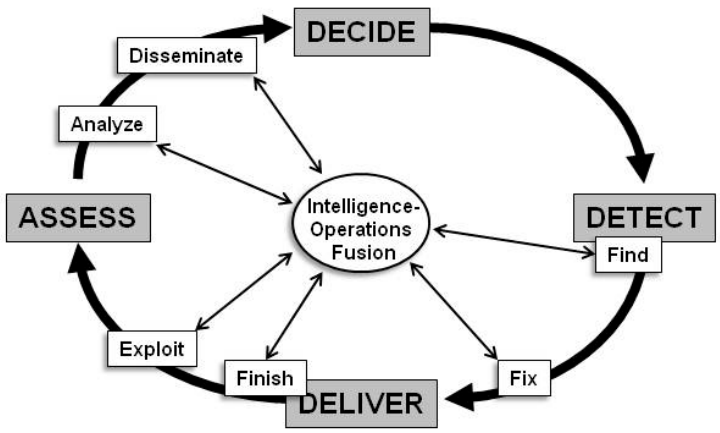

Figure 8. D3A and F3EAD combined. Conventional D3A is efficiently enhanced by tactical SOF elements simultaneously conducting F3EAD in a decentralized manner across an operational area (from FM 3–60 The Targeting Process, 2010).

The actual process SOF uses to intervene against targets is actually a combination of the conventional targeting process, referred to by the acronym D3A,* and actions derived from the SOF culture of bottom-up, decentralized operations. These operations are characterized by consistent information-sharing with all relevant friendly stakeholders and continuous refinements to planning. Referred to by the acronym F3EAD,† and as depicted in Figure 8, SOF conduct targeting within the conventional targeting process, particularly when a JFC exists in a given theater of operations. However, special operations commands mandate the fusion of operations planners and intelligence collection and analysis functions at all echelons from the JSOTF to the ODA. At the lowest levels—in the ODAs and AOBs—the same people who collect the information also analyze and disseminate the intelligence, and plan and execute the missions, then exploit any evidence or other information gained to inform their next targeting cycle.

* D3A is Decide, Detect, Deliver and Assess.

† F3EAD is Find, Fix, Finish, Exploit, Analyze, and Disseminate.

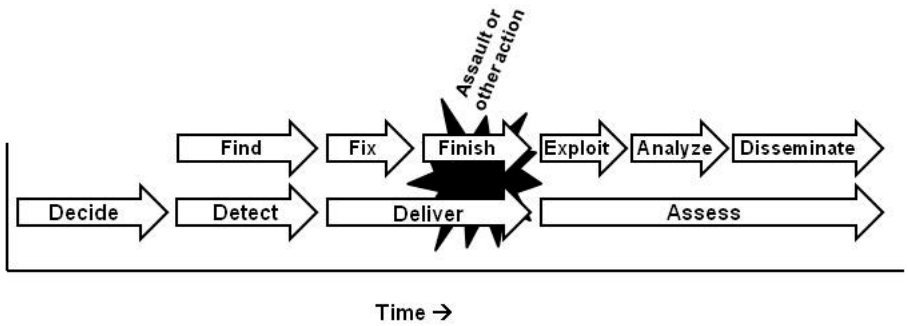

Figure 9. Comparative timelines for F3EAD and D3A processes in operations against a targeted high-value individual.

The target analysis methodology is intended to determine military value, priority of intervention (as compared to other potential targets) and the weapons and equipment required to efficiently inflict the appropriate amount of damage or influence upon the enemy. Input data required for effective target analysis include the commander's intent (i.e.: the commander's desired outcome), any data pertaining to the target structure, design and operation and consequences of various levels of diminished target system capability; personnel and equipment available for the mission (particularly any specialized equipment or expertise required to deal with a specific target, especially if it is unusually technical or complex), and the potential reactions of the enemy and other populations to different levels of diminished system output.[120] These factors are then used to create evaluation criteria to determine the relative merit of attacking or otherwise intervening against specific components or critical points of a targeted system.[121]

B. THE CARVER ANALYSIS TOOL

The actual method within the SOTP to evaluate and prioritize target systems at multiple levels is embodied in the acronym CARVER. The components of the process are: criticality, accessibility, recuperability, vulnerability, effect and recognizability.[122] Taken collectively, these components are meant to holistically evaluate the target system and the environment into which the target system is integrated. This method can be used at all three levels of war.[123] The analyst makes value distinctions based upon the commander's desired outcome in his stated intent. These values then become the measuring sticks which define not only the desired effects, but also the opportunities and constraints, indeed the lens, with which the operator-analyst disaggregates and assesses the structure of the target system. From this assessment comes the derivation of at least one course of action which, if successful, will bring about the desired effects. What follows is a brief explanation of each of the components.

Criticality is a multi-layered component of the SOTP. As the collective analysis descends through the levels of war (and the layers of systems, the target system, the sub-systems, the complexes and components of the target system), the information regarding the target system and its components becomes much more granular. Once a target system and the contained sub-systems and components are thoroughly understood, absolute and relative value distinctions between components of the target complexes and sub-systems can be established.

Accessibility is determined by the degree to which friendly forces or surrogates can make contact with the target actor or node to accomplish whatever the desired outcome requires. This component is traditionally thought of in terms of getting U.S. forces to a target site and to returning them to friendly territory again. In network terms, this is not necessarily so, though it may include such considerations particularly for kill or capture, or recovery missions. In the new context, it may refer to an ability to reach someone via the Internet or by transmission of a message or warning via clandestine personal or impersonal communications. As the term *access* is expanded to include targeted influence operations, the means can include idea leaders, mentors, and religious and other advisors.

The component *recuperability* refers to the estimated or known ability of a network to self-repair or adjust to damage inflicted by loss or disruption of an actor or node.[124] Two of the most expedient methods of recuperability are redundancy and overlapping responsibilities. Redundancy is merely having dual or more parallel roles or mechanisms, so any redundancy that is built into the network being analyzed, and affects the targeted sub-system, must be considered as detrimental to the mission and must be accounted for in the developed course of action. Responsibility overlap means that roles and functions are shared by more than one actor or mechanism and loss of one a few actors or nodes may not necessarily mean loss of the capability to the network.

Vulnerability is the fourth component of the CARVER analysis process. Vulnerability is a two-fold consideration. The first aspect is target-centric and the other is focused on friendly assets available for the mission. An actor or a network is vulnerable if it possesses a weakness that can be exploited. Traditionally, this is thought of as a person or a place being undefended or weakly defended from kinetic attack. In network methodology, vulnerability is widened to include trust issues, structural holes, principal-agent problems, and other symptoms of weakening structure or processes. The friendly force-oriented aspect concerns assets available and effective employment capabilities. If the friendly force is lacking either of these aspects, then the vulnerability will go unexploited. However, it may still be able to be monitored by the friendly force, in continued preparation for when assets or capabilities become available.[125]

The *effects* component can consume the greatest amount of the analyst's time, especially if the appropriate level of expertise is not available to assist with the analysis. "The target should be attacked only if the desired…effects can be achieved."[126] While the special operations targeting joint publication states that the intended effects may consist of any or all of the elements of national power (military, intelligence, diplomacy, legal, information, finance, economic)[127] and a strong emphasis is placed upon the effects on the local population, it does not focus on network effects. Three aspects of complexity come to the forefront with this component: non-linearity, ordering in dis-equilibrium, and self-organization.[*] The net effect of these aspects of complexity is that traditional linear cause-and-effect notions are replaced by "fractal" spreading of information and effects of intervention.[128] Here, fractal means that the internal and external edges of an organization do not conform to a line-and-block chart or the flow of information not conforming to predictable trajectories of diffusion, like a contagion. Tracing the flow of information through a complex network will show uneven diffusion across the graph with growth characterized by fits and starts as nodes of various centrality strengths receive and transmit the information.

---

[*] Refer back to Chapter 1 for discussion of the relevant aspects of complexity theory.

As information flows across the network, the actors will react to the information as they receive it. This will trigger reactions to the information in accordance with the role and position of the actor and his relations (mainly expectant trust) with his network neighbors.* At any given moment, there will be multiple waves of information flowing through the network simultaneously, with ripples of information and individual and collective reactions to the information constantly overlapping as they wash across the organization. In this manner, the network will constantly be in a state of informational and organizational dis-equilibrium. Actors will be continuously adjusting to each other's reactions to the information as well as to the information itself. Members will re-evaluate their trust levels in each other subsequent to each new bit of information shared. This applies to groups as well as individuals, with internal group dynamics (cohesiveness, centrality and levels of trust in the exchanges) between individuals coloring the net reaction at the group level. It is in this way that the net effects of any type of intervention into a system must be assessed and evaluated by the operator-analysts and planners.

The last component of the CARVER tool is *recognizability*. The concept of recognizability as applied to physical structures in the manual also have applicability in the human terrain—necessity to be able to visually differentiate the actual targeted actor from others. In dealing with the structure of relations across a network, being able to identify structural stress-points which, if able to induce failure, would cause collapse or disruption of the system in the intended manner is also very useful.† While it is vital to be able to physically recognize a targeted actor or node in a network, it may not always be feasible. What if the analyst has no physical description? Or, what if the analyst does not have information about the internal structure or membership of a group within a larger network, yet he must develop a plan to intervene against the group's influence? To answer these questions, we must look to the idea of information triangulation.

---

* Assuming the ability to monitor communication flow has not been undermined, the information flow patterns between actors will mirror the pattern of previous exchanges unless something changed about the relationship itself or communication capability.

† While the current manuals give a nod to information operations targeting, it is computer network-focused and does not explicitly address the human terrain or dark network intervention.

Data triangulation is a method to overcome a lack of direct access to information by compiling and aggregating information from different information sources surrounding the targeting problem.[129] What it lacks in precision about the problem in question, it makes up for in knowledge surrounding the problem, thereby gaining intimate detail about the social patterns and trends around the problem and insight into how the problem itself influences its environment, and vice versa. This is not unlike the manner in which scientists study black holes; while black holes are invisible due to the inability of light and other electromagnetic radiation to escape the hole's gravitational pull and be detected by telescopes, astronomers are able to measure the effects of the tremendous forces at work by watching the stars and other matter in the vicinity of the black hole behave in accordance with physical laws *because of the influence of the black hole*.[130] In network terms, this analogy equates to monitoring the actors in the network neighborhood around the mystery actor or group for influences from that actor of group. Over time, patterns and trends can be detected and compared so reasonable expectations can be derived about future influences and probable target and target neighborhood reactions to intervention and, thus, plans to eliminate or mitigate the emergent influences can be developed. While this idea may or may not assist in creating a Special Operation Target Intelligence Package for a direct action (assault) mission, it will certainly assist in development of targeting guidance for influence operational planning or in constructing a plan for further intelligence collection.

SOF use the CARVER method at all three levels of war, in exactly the same manner, but using information detail appropriate to the level of analysis. For CARVER to be efficiently used and targeting decisions to be understood, each echelon may define the values *at that echelon* in absolute terms. Those values must be understood across all levels of analysis and must be in accordance with the commander's intent, and agreed upon expert assessments of friendly force capabilities and limitations, knowledge of the target itself, the larger systems in which the target is embedded, the physical terrain, the weather, and other environmental factors. Figure 10 displays a notional CARVER value rating scale for use across the three levels of analysis. Any discrepancies in or new information concerning any of the above factors must be integrated into the analysis of all echelons. This may require partial or entirely new analysis, depending upon the assessed impact of the new information. The impact of first-hand knowledge of critical aspects of the target and target systems cannot be understated.

Another peculiarity of SOF is the ability to gain or recruit the expertise and technical resources to affect such depth of analysis. This highlights another difference between special operations and the conventional military, as the conventional military's approach to evaluating options frequently consists of force ratios (comparing numbers of friendly and enemy aircraft or tanks, for example) and "troop-to-task" analysis of numbers of assets as compared to the number of targets capable of being attacked by types of weapons systems. Conversely, SOF do not possess large numbers of troops or aircraft, nor are they rapidly regenerated in the event of casualties, so they necessarily must be selective and deliberative in their targeting and risk management.

When each echelon completes its analysis, the lower echelon refines its information requirements and then completes its own analysis. Some portions of analysis and planning are completed concurrently between the echelons out of necessity but some resources are scarce (such as expertise in some technical aspects of a target system) and require sharing. Figures 11, 12 and 13 display CARVER matrices developed for the strategic, operational and tactical levels of analysis against a notional hostile state.

CARVER VALUE RATING SCALE (NOTIONAL)

VALUE	C	A	R	V	E	R	VALUE
5	Loss would be mission stopper	Easily accessible. Away from security	Extremely difficult to replace. Long down time (1 year)	Special operations forces definitely have the means and expertise to attack	Favorable sociological impact. OK impact on civilians	Easily recognized by all with no confusion	5
4	Loss would reduce mission performance considerably	Easily accessible outside	Difficult to replace with long down (<1 year)	Special operations forces probably have the means and expertise	Favorable impact; no adverse impact on civilians	Easily recognized by most, with little confusion	4
3	Loss would reduce mission performance	Accessible	Can be replaced in a relatively short time (months)	Special operations forces may have the means and expertise to attack	Favorable impact; some adverse impact on civilians	Recognized with some training	3
2	Loss may reduce mission performances	Difficult to gain access	Easily replaced in a short time (weeks)	Special operations forces probably have no impact	No impact. Adverse impact on civilians	Hard to recognize. Confusion probable	2
1	Loss would not affect mission performance	Very difficult to gain access	Easily replaced in short time (days)	Special operations forces do not have much capability to attack	Unfavorable impact. Assured adverse impact on civilians	Extremely difficult to recognize without extensive orientation	1

Note: For specific targets, more precise, target-related data can be developed for each element in the matrix.

Figure 10. A notional CARVER matrix rating scale defining values to be used later in the process. These values are drawn from data about friendly forces' capabilities, the target itself, the larger systems in which the target is embedded, and other environmental factors, as well as the unit commander's preferences. From JP 3-05.2 Joint TTPs for Special Operations Targeting and Mission Planning, 2003.

SAMPLE STRATEGIC CARVER MATRIX APPLICATION

TARGET SYSTEMS	C	A	R	V	E	R	TOTAL
Bulk Electric Power	5	3	3	5	5	5	26*
Bulk Petroleum	5	3	5	4	3	5	25*
Water Supply	3	5	3	5	5	3	24*
Communication Systems	3	4	5	2	2	2	18
Air Transport	1	1	3	1	2	2	10
Ports and Waterways	1	1	3	1	1	1	8
Rail Transport	2	4	4	1	4	3	18
Road Networks	1	5	3	5	2	5	21

*Indicates target systems suitable for attack. In this example, the Bulk Electric Power target system has been selected.

Figure 11. An example of a strategic-level CARVER matrix. From JP 3-05.2 Joint TTPs for Special Operations Targeting and Mission Planning, 2003.

SAMPLE OPERATIONAL CARVER MATRIX APPLICATION							
TARGET SUB-SYSTEMS	C	A	R	V	E	R	TOTAL
Generation	5	3	4	3	5	4	24*
Transmission	2	5	2	5	2	5	21*
Control	3	1	4	1	3	3	15
Distribution	2	4	2	4	2	3	18
*Indicates target sub-systems suitable for attack. In this example, the Bulk Electric/Generation sub-system has been selected.							

Figure 12. An example of an operational-level CARVER matrix. From JP 3-05.2 Joint TTPs for Special Operations Targeting and Mission Planning, 2003.

SAMPLE TACTICAL CARVER MATRIX APPLICATION							
TARGET COMPONENT	C	A	R	V	E	R	TOTAL
Water Intake	3	5	1	1	5	4	19
Water Filters and Pumps	5	4	5	4	5	3	26*
Ion Filter	2	1	1	1	5	1	11
Pre-heater and Pumps	5	2	4	3	5	2	21*
Air Intake	2	1	1	1	5	1	11
Blowers	2	2	1	1	5	1	12
Barges	1	5	1	4	1	5	17
Docks and Oil Pumps	3	5	2	3	1	4	18
Storage Tanks	1	4	1	4	1	5	16
Pre-heaters and Pumps (Fuel)	5	4	4	3	5	4	25*
Boiler	5	4	5	3	5	4	26*
Turbine/Generator	5	3	5	4	5	5	27*
Transformers	3	4	2	4	5	4	22*
Power lines	5	1	1	1	1	1	10
Switching station	2	1	1	2	1	1	8
*Indicates target components suitable for attack. In this example, the Bulk Electric /Generation/ Turbine target has been selected.							

Figure 13. An example of a tactical-level CARVER matrix. From JP 3-05.2 Joint TTPs for Special Operations Targeting and Mission Planning, 2003.

The difference in information requirements and analysis outputs are evident in the size and detail of the above CARVER matrices. The strategic CARVER (Figure 11) compared only massive, national-level infrastructure systems such as transportation, bulk petroleum and communications. Of those systems compared, the analysts selected the national electric power grid, and would have directed operational level analysts and planners to analyze the systems within the hostile state's national electrical systems.

The operational level CARVER matrix compared the subsystems as depicted in Figure 12. These analysts and planners concluded that the power generation subsystem was most feasible for attack, and directed the tactical planners to analyze the tactical subsystems and components within a particular generation plant for possible targets of a direct action assault. This plant is a hydroelectric dam.

These tactical planners developed a CARVER matrix of their own (Figure 13) to determine the subsystems and components of those systems for destruction. They selected the turbine generators as their most feasible target, followed closely by the boilers, and the water filters and pumps, and then other components. As modern hydroelectric dams and the computing and mechanical systems that run them are extremely complicated, there is yet another decision the planners must make to execute this mission: how to attack the turbine generators.

Among the options available to special operations are 1) unilateral direct action, 2) train and employ a human agent to carry out the on-site tasks, or 3) some combination of those two. Figure 14 depicts the addition of the social side of the equation: the bureaucracy and staff of the dam itself.

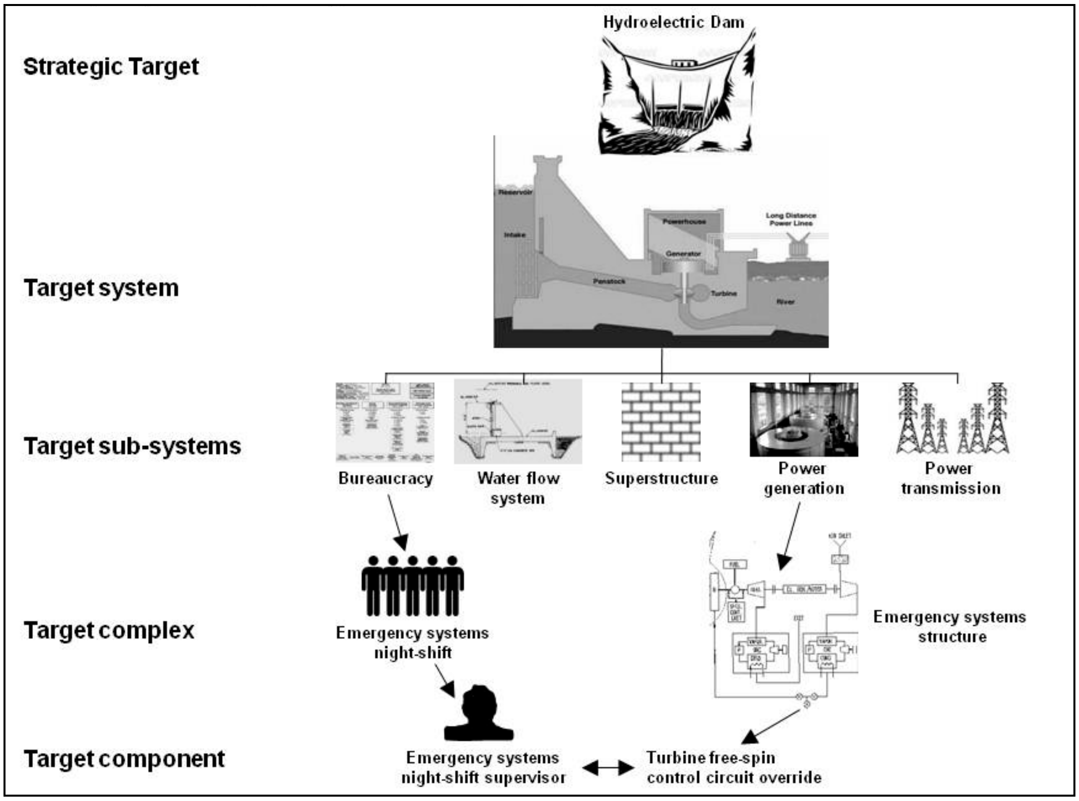

Figure 14. A hypothetical hydroelectric dam system of systems. In special operations, technical and human systems must be considered together. While the military expertise resides with in the special operations team, the on-site technical and social expertise resides only within the native staff.[131]

Now the planners have the information necessary to provide the commander—as the primary decision maker—a range of options to accomplish the mission. As demonstrated, the information and decision requirements vary from level to level, and correspond to the level of analysis being performed. The above discussion of the SOTP should bring out the conclusion that, while the SOTP was designed without social networks in mind, its treatment of a target as a system possessing and interacting with parallel systems and sub-systems within a larger environment also, successfully encompasses the major concepts of netwar. And, for what is does not specifically address, it allows for re-interpretation and expansion of the components to include practically all assessment and evaluative requirements to successfully address SNA input and intervention strategy information requirements. While the military has applied the SOTP and CARVER to irregular warfare for a few years now, it has not yet been combined with social network analysis to effectively combat terrorist or insurgent networks. Thus, the full potential of application to irregular warfare has not been realized. The next chapter is an introduction to SNA.

IV. INTRODUCTION TO SOCIAL NETWORK ANALYSIS CONCEPTS AND METHODS

Social networks are individuals and groups interacting to achieve some goal or fulfill a purpose. Networks are constantly expanding and contracting (increasing and decreasing in membership) for many purposes: to gain, disseminate, and respond to information; to collect and distribute resources; to make money; to cope with threats; or to create new knowledge.[132] The field of study dedicated to measuring and understanding patterns of position and power is called social network analysis, or SNA. This chapter will introduce basic SNA concepts and processes in terms of dark networks sufficient to understand the linkage to the special operations targeting process, and to inform a combination of the two concepts to make a more effective tool for use in irregular warfare.

SNA determines relative levels of power and influence according to members' social ties. That is to say, SNA is a tool that can be used to understand an actor's level of access to information and placement within a group or organization of interest to the analyst. While a primary desired outcome of SNA is "detecting and interpreting patterns of…ties between actors,"[133] it is also intended to provide insight into characteristics of entire networks. SNA allows analysts to understand qualities of the network as a whole, as well as the qualities of individuals. The term "actor" applies to individual members of a network or to groups that interact with other groups, or between groups, within or between organizations, and may be extended to describing inter-state patterns in international relations. SNA measurements can indicate inter-group dynamics and social processes above the individual level.[134]

A. KEY TERMS

To use SNA, as in other fields of study, there is a family of terms that must be consistently used. The most fundamental of these are:

Node. The basic unit of a network, a node (also called a vertex) can be a person—usually termed an "actor"—or an object, place, attribute, event, or idea, depending upon the analysis under way. Nodes are uniquely named to prevent confusion.

Link. A link is a tie between two nodes indicating a relationship. On a graph, a link is a line drawn between two nodes. It may be valued as positive or negative, directed from one node to another, or otherwise valued to indicate the strength of relationship between nodes. A link is defined by its end points.

Path. A path is a series of links between nodes in which no single node occurs more than once. It is defined by its end points, or by a set of points to differentiate it from other paths. A path is a tool used for network-wide measurements and for descriptions of a mechanism, or a set of relationships deliberately arranged. If there are more than two nodes with links between them, then multiple paths may be present.

Graph. A graph is the visual layout of a network's nodes and links. A graph may depict the smallest of networks, those of two or three nodes, or a large network consisting of hundreds or thousands of nodes. Nodes are distributed across the visual field by various mathematical formulas.

While terms must be universally accepted, definitions can be relaxed to account for data gaps or other sources of systemic errors caused by strict definitions. This type of judgment is significant for analysts to understand and articulate, especially when fighting dark networks. However, using definitions and methods that are too relaxed may lead to new sources of systemic error and skew later analysis. In this manner, SNA requires balancing the science of quantitative analysis with the art of understanding the qualitative dynamics of the human terrain. Other terms will be introduced as required later in this and following chapters.

B. SNA AND DARK NETWORKS

Dark networks are a subset of social networks characterized by their illicit nature. Dark networks may function similarly to other "bright" or legitimate networks but are obscured with intentional secrecy or deception. In terms of observation and analysis, secrecy changes everything.

The works of Simmel,[135] Erickson,[136] and Herdt[137] tell us that groups maintaining secrecy are different from other groups, both in structure and in behavior, and spend enormous energy and resources to maintain their secrets. This is primarily because of how the group relates to the surrounding environment—members must decide whom to allow into the fold, and whom to exclude. Secrecy changes much of what members of dark networks do on a day-to-day basis, and much of their time is spent making up for clumsiness or mistakes. Ironically, it the very secrecy that protects dark networks that also limits their growth and development.[138]

What makes a network dark or illicit? The evaluation of a network as being licit or illicit requires a look at the surrounding environment—it depends upon who controls the physical space in which the network is operating and whether the network is operating in compliance with or contrary to legal or social norms. If the network members are functioning contrary to the laws and norms of the local environment, then they must maintain some degree of secrecy or suffer punishment or expulsion, thus their network is a dark network. Further, every location in which the network exists is not uniform in laws and local norms and the network members modify their behavior accordingly as they pass through or operate across boundaries and cultures. Thus, a primary benefit of ungoverned spaces to a dark network that finds a home there is that it may use it as sanctuary, thus saving resourcing and energy for the places where members must maintain cover and conceal their actions. Correspondingly, analysis of networks in their varying social contexts cannot be monolithic either.

There may be some physical or virtual places where a network can operate in the open and other places where it must remain dark to avoid repression or attack. Dark networks, then, are not necessarily confined to those places where it must operate in complete and utter secrecy. The mere risk of a threat to its purpose, membership, or existence is sufficient for it to remain a dark network to survive and function. It is this secrecy and inherent threat to the investigator which demands particularly rigorous methodologies for discovery and tracking that are currently uncommon in traditional SNA research. This is where the primary contributions of special operations and intelligence activities can supply the information necessary for SNA of dark networks.

C. ANALYTICAL ASSUMPTIONS

Like every intelligence and planning process, SNA is subject to limitations which require using assumptions to overcome. In general, there are three basic planning problems with SNA that have an especially severe impact on analysis of dark networks:

Incomplete information. Not everything that influences network formation or flows will be apparent to the analyst. When analyzing dark networks, such as insurgencies, terrorist groups or underground movements, this is compounded by secrecy and deception.

Fuzzy boundaries. When collecting and analyzing data concerning a dark network, the limits of the network are likely unknown and variable, and dependent upon many factors, not the least of which are the analyst's desired outcomes of the investigation. As information accumulates, the analyst must determine exactly whom to include in the network and whom to exclude.[139] Not only is this a function of the level of analysis, but also of the fact that people are members of multiple layers of networks simultaneously and may be key players in some social settings but peripheral in others.

For example, an actor can be a patriarch of a kinship network, a middle-level manager in a workplace network, an "on again-off again" golf buddy in a friendship affiliation network, and a non-practicing member of a religious group. Including more or less data in the scope of the investigative process will change the outputs of the tools used to assess and evaluate the target network. Using too much or too little data can skew findings and perhaps lead analysts and planners in the wrong direction.

Dynamic nature of networks. Social networks are always changing. Membership waxes and wanes and internal organization, information pathways, and distribution of resources, responsibilities and tasks are constantly adjusting to internal and external influences. Actors may join a network but may remain inactive until certain conditions or events trigger their activation. Or, members may participate in the beginning of their experience, but their participation may taper off or terminate over time. Thus, total membership may not always be meaningful, but it depends on the goals of the analysis. It remains up to the analyst to decide when and how an actor counts and in what context.

As a corollary, an undesirable but expected outcome of investigation into dark networks is that, upon discovering that it is a target of an investigation, network members will take measures to adapt to the investigator's activities and disappear from view. If discovered, an investigator risks negating some or all of the known data about the network. Thus, to avoid threats to the investigation, it behooves the investigating element to conceal its own activities to the utmost.[140]

For analysts and planners, there are many useful aspects of SNA output information about dark networks and social networks in general, but what is required of those analysts and planners from the outset is a thorough recognition of the concepts behind the methods and outputs so the appropriate input data can be collected. John Scott's handbook of SNA presents an easy to understand breakdown of types of sociological data collected for study: relational, attribute, and ideational.[141] This thesis explores relational and attribute data of actors as relevant to understanding the match between SNA and the SOTP, but ideational data can be important for understanding the shape and flow of ideas and how ideas are related.

D. DOING SNA: COLLECTING INPUT DATA

The concepts associated with the conduct of SNA data collection, analysis and interpretation, and dissemination constitute the remainder of this chapter. Using specific input data and analytical software, SNA output data can then be depicted graphically, analyzed mathematically, and used to build a framework for designing an intervention strategy. A planner can apply the same concepts for formulating an assessment strategy to measure progress.

While positional and relational data comprise the majority of SNA input data, they do not stand alone as there are geographical and temporal[*] relationships to the data as well. Most depictions of social networks are merely a snapshot in time in the life cycle of a network; the membership and structural changes in a network over time must be explicitly described in SNA. For example, a person who joins a network does so at a

[*] Temporal information is time-oriented data describing arrival, departure or duration of some relevance.

specific time, which is after the previous members joined the group and before any subsequent members joined. Thus, if an analyst were to be looking for participants in a certain event that took place at time *T*, then the analysis would specifically exclude any members of the network who had not yet joined by time *T*. Or, if that same analyst was looking for participants in the same event, then he could exclude those members of the network who are known to be in other regions or under surveillance at the event time as they could not have participated in the actual event. It is this kind of assessment that, while it may be intuitive, is a necessary element of analysis and that data must be explicitly accounted for during analysis.

On relations between actors, a common relationship considered practical and worthy of analysis is direct communication, followed by known participation in a specific event, and then by known membership in a formal or informal organization.[142] An example of the first is reporting that actor A talked to actor B by phone. An even more precise disaggregation of the input information would be that actor A used phone X to call actor B at phone Y at time *T*. Thus, we have five data points from one bit of information. Depending upon the level of sophistication of the technology at the analyst's disposal, he could even have geographical data[*] regarding the phones' locations at the time of the call as well as actual ownership data for the phone numbers leading us to seven or nine data points from this one collection instance.

Another aspect of communication, specific to the more sophisticated dark networks, is the use of tradecraft[†] for clandestine communication procedures and methods. Tradecraft can be both technical and non-technical in nature, and the number and variety of techniques employed is limited only by the creativity, resourcefulness, daring and skill of the involved parties. One example of technical tradecraft is the embedding of encrypted messaged in image and other types of files that are emailed or posted on Internet websites for retrieval by another Internet user located anywhere in the

[*] So-called "geo-tagging." Another form of this capability is accessible to civilians via the GPS functions on current "smart" cellular phones. The physical location of photos taken with smart phones and directly uploaded to the Internet can be determined by reading the meta-data embedded in every digital photo.

[†] Tradecraft is a term for the employment of methods and procedures to conduct operations while under, or suspicion of, surveillance or suppression by opposing forces or agencies.

world. An example of non-technical tradecraft is the use of "dead drops" where messages are concealed at specific, secret locations known only to the sending and receiving parties who visit the site at different times to prevent any direct association by an outside observer. In this manner, depending upon the relative skills of the competing entities, the direct communication links may not be visible to an observer. Sometimes face-to-face conversations between two skilled, but unfamiliar agents are the most secure form of communication because of the apparent randomness of the event.

Direct communication is only one of many types of relations between actors. While direct communication may seem to be the most likely avenue for transmission of information, such is not necessarily the case with the advent of the mass media and, in particular, the cyber domain. One term for this phenomenon is "open-source warfare," or OSW.[143] The key characteristics of OSW is that there need only be a medium for broadcasting of information, preferably in a persistent state, so otherwise un-connected actors can receive the same information. In a concept taken from the insect world, John Robb describes this as "stigmergy" or the ability to transmit and receive signals without direct connection.[144] Television, radio and the Internet are the prime examples of OSW media, but just about any other similar broadcast media can accomplish the same effect as long as the intended audience is able to receive the message.

Aside from communication and influence, affiliations and attribution data often provide grounds for analysis of useful patterns and trends between actors and groups. Commonalities in life experiences, education, geographical or physical proximity, community membership, and other significant forming experiences provide data regarding attributes of actors that may provide insight into previously unseen patterns and between actors. In certain circumstances, such as counterinsurgency and counterterrorism operations, key players attending an important meeting or other collaborative event will be the most meaningful attributional data.[145] Such relevant historical information may go back years and require a substantial amount of research to be of use.

E. DOING SNA: OUTPUT DATA AND ITS USEFULNESS IN INTERPRETING FOR PATTERNS AND INDICATORS.

Understanding the expression and interpretation of SNA data output is equally important to understanding how input data is collected, recorded, manipulated and measured. SNA data—both input and output - can be considered in two modes: 1-mode and 2-mode. 1-mode data is used to study relations between like actors—people to people, for example. 2-mode data is used to analyze the relationships between two unlike but connected objects—such as people to places, places to time, etc. When combined, 2-mode data can become attributional data to give context or strength to the1-mode direct relations data. Similarities in attributes among actors who are related can give credibility to otherwise sparse information concerning direct relations, but it all must be taken in context.

There are two basic categories of SNA output data: graphical and numerical. Graphical expression (Figure 15) is accomplished by producing a graph of a network using symbols for nodes to represent individual actors (persons or groups of people, depending upon the level of analysis being conducted), and lines to depict the relations between actors. While manipulation of symbols and other visual indicators of measurements may frequently be best expressed visually on a graph or chart of a network, sometimes the nuance of relative strength or direction of relations is better expressed in numbers.

Numerical SNA output information is generally laid out in tables according to the type of data and measurements used. These tables can include variations of those measurements in sometimes long, parallel lists of numbers that mean little to an observer until analyzed with Microsoft Excel or other data manipulation software. The importance of the analytical capabilities of Excel or other software cannot be overstated, but the depth of analysis must not outrun the quality of the input data, given Sparrow's three analytical assumptions.*

* Incomplete information, fuzzy boundaries and the dynamic nature of networks.

A-B
A-D
A-E
A-F
A-G
A-H
B-A
B-H
C-E
C-F
C-G
C-H...

	A	B	C	D	E	F	G	H
A	0	1	0	1	1	1	1	1
B	1	0	0	0	0	0	0	1
C	0	0	0	0	1	1	1	1
D	1	0	0	0	0	1	1	0
E	1	0	1	0	0	1	1	1
F	1	0	1	1	1	0	1	1
G	1	0	1	1	1	1	0	1
H	1	1	1	0	1	1	1	0

Figure 15. Three types of displays of SNA data: graphical output (left), a portion of a relational data table (center), and matrix data (right) used to make graphs similar to the one on the left.

With regard to designing graphical output, the options for using symbols to depict important attributional, relational, temporal or geospatial data is limited only by the analyst's creativity and sophistication of the systems used to conduct the analysis. Currently, symbols are limited to what our SNA software allows. But it really depends on what is useful and necessary for the analyst to know and how to describe what he knows.

1. Direct Relations

The same decisions concerning displaying sufficient information graphically apply to how relations between actors are depicted. If all that is important is that a link between actors exists, then a simple line suffices. If the amount of communication is important, and the direction (incoming and out-going) is also important, then such could be expressed in a directed graph, or di-graph, with some depiction of increased value or strength to that link—such as a thicker line or a numeral adjacent to the line. If the collaborative or adversarial nature of a relationship is important, then a positive or negative value could be assigned. In short, the essence of graphical representation is to say with pictures what could be a thousand words. See Figure 16.

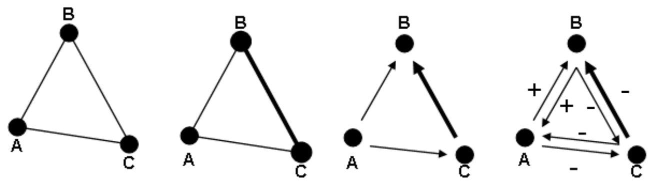

Figure 16. Graphs depicting increasingly sophisticated depictions of a triad network. Left to right, a simple graph showing nodes and links, a valued graph with the B-C link having a higher value, a di-graph with a higher-valued B-C link, and a di-graph showing an A-B coalition against C.[146] Triads are critical to understanding some of the most fundamental of social dynamics like choices and exchanges.

The expression of positivity-negativity and relative strength of ties within social networks has significant implications for interpreting SNA data with regard to assessing trust and potential future interactions between actors. Because "trust is a bet about the future contingent actions of others,"[147] a valued link may be useful to an analyst because it gives insight into the nature of a relationship and future transactions. It follows that if a long-lasting, strongly positive tie between two actors indicates a high level of trust to act favorably toward each other, then it follows that an equally strong and long-lasting but negative relationship may also indicate that a high level of expectation anticipation between the two actors to behave negatively toward each other. This gives rise to indicators of coalitions and factions within social networks. Some of these groupings have specific qualifications and definitions.

2. Dyads and Triads

David Krackhardt has explored George Simmel's[148] and Mark Granovetter's[149] lines of thought concerning dyadic and triadic dynamics—or a range of a person's choices when analyzed as a member of groups of two or three direct and mutual relationships. Dyads are direct relations between two people and may be characterized here as strong or weak, with each member having power to control the relationship. Granovetter's work on the strength of weak ties revealed that one person's distant relationship with another may provide critical access to new information and resources, as well as access to distant groups of people, and may make relatively weak ties more advantageous than a whole range of strong ties, particularly over time.[150] Thus, a dyad, as the smallest form of network relations, may prove to be extremely strong and safe as long as the two members can get along.

Dyads are also extremely vulnerable. When there is only one network option available to a person or group, then the actor to whom the group is connected becomes extremely powerful. Since all information or resources must flow through that one node, then the role of that node can take on shades of gatekeeper, coordinator, representative, liaison or broker.[151] This dynamic can wield significant power over large groups connected only by a single dyadic relationship.

In triads, or relations of three mutually-connected members, Krackhardt defines a Simmelian tie between two people "if they are reciprocally and strongly tied to each other and they each reciprocally and strongly tied to a mutually-shared third person."[152] Krackhardt characterized Simmelian ties as "super strong and sticky" to describe their resilience and durability over time. While these kinds of relations can be an expression of trust based on duration or history of the relationship, frequency of interaction, affinity and reciprocity, they are also a source of other factors shaping a member's behavior. These are 1) reduced individuality, 2) reduced bargaining power, and 3) enhanced conflict resolution resulting in conformity to the larger group's expectations.[153]

The critical instrument derived from these ideas is that people's choices and actions are, at least in part, determined by their social network's structure. When an actor is a member of a dyad only, he has power to sever the relationship, but both parties lose access to what the other brought to the relationship. When actors are members of a Simmelian tie, the behavior of all three is modified and shaped by the choice each possesses in the presence of the third member. That is, each member knows that if he breaks ranks with the others, they will be able to maintain their relations without him. Exclusion is punishment.

The power and constraints within dyads and triads are very important. Strong, unique dyadic ties are very powerful but vulnerable to manipulation by one or the other member. Triads can lead to successful group behavior, but too many triads can lead to redundant (non-new) information pools and stagnation. The implications of these tandem theories are instrumental to shaping and attacking dark networks as structural sources of power and access to information or resources may be used to force entry into a dark network's neighborhood and coerce a group to change its structure or activities.

3. Structural Holes, Secrecy and Synchronization

Ron Burt describes structural holes as "disconnections" in social network structure to be filled by those seeking advantage in associated transactions.[154] While the emphasis in most academic literature for structural holes is for the implementation and growth of social capital in market and corporate contexts, the idea certainly applies to dark networks. There are significant information and control advantages for the actor who brokers or closes the gap between two other parties in need of mutually beneficial exchanges. The information advantage comes in the form of access, timing and referrals. That is to say, an actor who bridges a structural hole has access to information not available to all members, awareness of information before others get it and status in other members' minds for information and resource garnering.[155] The control advantages are implicit in the uniqueness of this position: the actor can choose what to share. Granovetter's strength of weak ties makes an important contribution to this kind of relationship building as weak ties close the gap between non-redundant sources of information.[156]

For dark networks, structural holes are very special considerations. The imperative of secrecy demands a protective shell of structural holes for the mere necessity of limiting the flow of information to only those intended. This applies both externally and internally to the network (i.e.: compartmentation of functional cells or mechanisms to protect the larger network from compromise of one or more of those sub-groups). Holes in networks diminish their density and detract from their cohesion measurements. That makes identifying the boundaries of a network even more difficult, since density, cohesion, and blockmodeling[157] may be used as indicators of network membership boundaries. Alternatively, a group surrounded by structural holes with few connections to outside actors, may very well be an easily identifiable network. Employment of gatekeepers, brokers, or liaisons elongates information pathways and diminishes centrality and other measurements that could bring key players to light.

Attrition of non-redundant cells or members from attacks or compromise creates structural holes. The loss of a non-redundant broker or gatekeeper connecting two or more cells or within a chain can mean the loss of communication and, therefore, synchronization of actions. Due to the illicit nature of dark networks, recruiting replacements is difficult and communications conducted by highly specialized tradecraft techniques are not easily re-established. Thus, dark network members must maintain a balance between secrecy and synchronization.

4. Network Density

The concept of social network density, and variations of density, can be displayed by graphical representations as well as mathematical measurements. Density refers to the volume of links between nodes in a network. It is a computation of the number of actual links (provided by the input data) as compared to the total number of possible links, given the number of nodes presented in the input data. Without introducing mathematical formulas, network density reflects the quantity of relations of members within a network and some qualities about the network as a whole.[158] Mathematically, density is measured on a scale between zero and 1.0, with the maximal value indicating complete density where there can be no more ties established. Visually, variations in density can only be detected by extreme differences or in very small networks (see Figure 17). To measure density across very large networks, SNA software must be used.

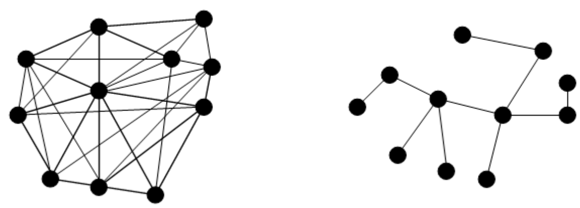

Figure 17. An example of a relatively dense network (left) and a relatively sparse, or low density, network (right). There are far more triads in the denser network, which could have behavioral implications for members.

Key to understanding the density measurements are the variations in density, which show evidence of sub-groups, cliques, and core-periphery boundaries in networks.

Changes in density across a network can also indicate benign demarcations of lesser-connected social groups within the larger network or gaps in intelligence. If the data are reliable, changes in density could represent schisms or other meaningful sub-groupings of network members. Graphically, density changes are depicted by a portion or portions of the network which are very highly-interconnected—representing a denser core or sub-group—and other areas which are less interconnected and show fewer ties between actors. The impact of Figure 18 should be not only the visual difference in density of ties between actors, but also the difference in the number of Simmelian options by way of the number of possible triads available to each member of the core vice the number available to members of the periphery. Thus, higher density measurements increase the likelihood of resilience and durability of the network as a whole, due to the internal maintenance effects of the many Simmelian ties available to members of a denser network. There may also be implications for potential isolating effects of a network core or other subgroups since the number of triads diminishes as we cross the boundary from core to periphery.

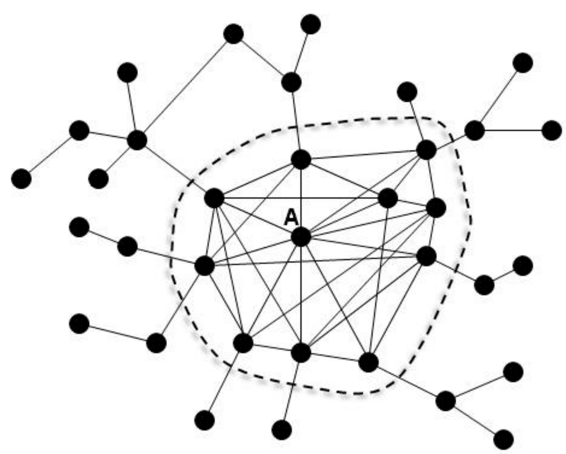

Figure 18. A network graph demonstrating the variation in density between the highly-interconnected core (inside the dashed circle) and the lesser-connected periphery. In very large networks, subgroups may not be so easily determined, but the difference in volume of network options available to members is significant.

5. Subgroups

Moving beyond dyads and triads, definitions of subgroups identified in SNA range from very strict to fairly relaxed and adaptable to a given dataset. Subgroups exist based on ties amongst network members (as in one-mode networks) and are named according to their method of measurement: cliques, cores, and clusters. While there are several names within those categories for the various subgroups, the subgroups with built-in flexible definitions may be of the most use due to the three analytical assumptions from earlier in this chapter. Being able to relax or otherwise modify the definitions changes the parameters of the mathematical formulas used and allows the analyst to experiment with the data to ensure honest analysis that answers relevant questions about the network.

F. DOING SNA: CENTRALITY MEASURES AND THE KEY PLAYER PROBLEM

Measurements of centrality are at the heart of SNA and give indications of network members who are relatively more knowledgeable and powerful than others. One term for those actors of relative importance is a Key Player.[159] Centrality measures are some of the tools useful for identification of Key Players, or those network members valued above other members. This is not absolute, however, as a member's position within a network is merely indicative of access to an information pool and placement within a field of possible informational streams. The previous concepts of trust and role, together with access and placement are critical factors in determining the power of a specific actor in a network. It is important to remember that these measurements provide the quantitative evaluation of actors, and the analyst must apply a qualitative filter based on facts or valid and necessary assumptions.

1. The Key Player Problem

The Key Player Problem, as defined by Stephen Borgatti, has two modes: first is finding the Key Player who is maximally connected to the most relevant information paths in the network (known as KPP-Positive) and second is identifying a Key Player according to the overall network's dependence upon him for cohesion (called KPP-

Negative). KPP-Positive is intended to focus on the actors who are best-positioned for information dissemination across the network. KPP-Negative is to determine which actor or actors are uniquely positioned so as to be the most damaging if removed from the networks in which they are embedded.[160] Depending on which mode you are using and the purpose of the analysis, different types of centrality are more useful, but all can provide information about the structure of the target network and the location and identity of key players within.

2. Centrality Measures

There are several types of centrality, and more are being developed, but the most commonly used are degree, closeness, betweenness, and eigenvector centrality. Many of the newly-developed measurements are combinations or refinements of these basic measurements.

Degree centrality is a measurement of the number of direct ties an actor has to other actors, or how many people someone knows. It indicates the potential for direct communication activity.[161] An actor with high degree centrality can be called a "hub" due to the graphical representation resembling a wagon wheel with the hub–the actor–in the middle of radiating spokes to other actors. This is also referred to as "local" centrality because it is a measurement of all the nodes based upon their 1-degree network neighborhood. Referring to Figure 19, actor A has the highest degree centrality, because he is directly connected to more members than anyone else in the sample. Actors F and G are the next highest-scoring members.[162]

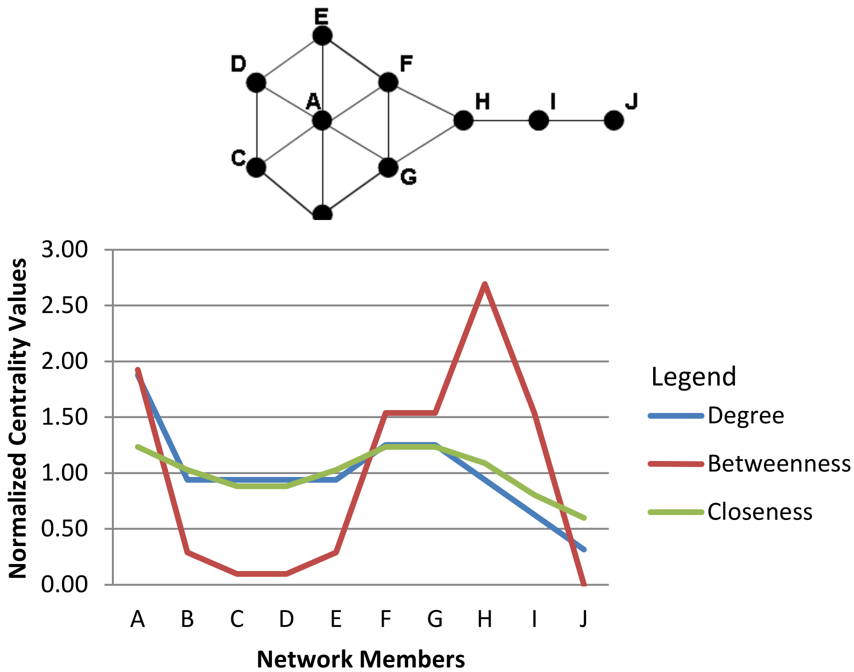

Figure 19. A kite graph for demonstrating centrality measurements and the corresponding centralities. In the lower chart, actor A has the highest degree centrality, actors A, F and G have the highest closeness centrality and actor H has the highest betweenness centrality.

Closeness centrality measures the distance from any node to the edge of the network. As such, it provides a glimpse of "global centrality"[163] or how central an actor is to the overall network. It is indicative of who may be most aware of information and events across the network.[164] Actors F and G have the highest closeness centrality because they are the closest to all other members.

Betweenness centrality of a node is a measurement of how many possible information pathways are intersected by that node. In the same figure, actor H has the highest betweenness centrality because all nodes must pass information through him in order to reach the far left and right boundaries of the illustrated network. A nodes betweenness centrality may indicate a potential point of control of information flow across a network.[165]

Eigenvector centrality. The eigenvector centrality measurement came about because network researchers recognized that sometimes an actor's power comes not from his own reach or volume of relations, but from that of whom he knows. In lay terms, it's all about who you know and the number of their direct connections.[166] In Figure 20, actors K, N, S and T come out with a very high eigenvector centrality score. Actors from J leftward all rate very low, and those actors surrounding that core group all rate in the median. The low-ranking members do not have network neighbors who know very many people, especially compared to the actors in the more populous side of the graph. So, if an actor is structurally positioned, trusted, and accessible as K, N, S and T are, then he or she will be a critical asset to the two groups located on either side. The implications of power through situational awareness and control for a core of members like this are obvious.*

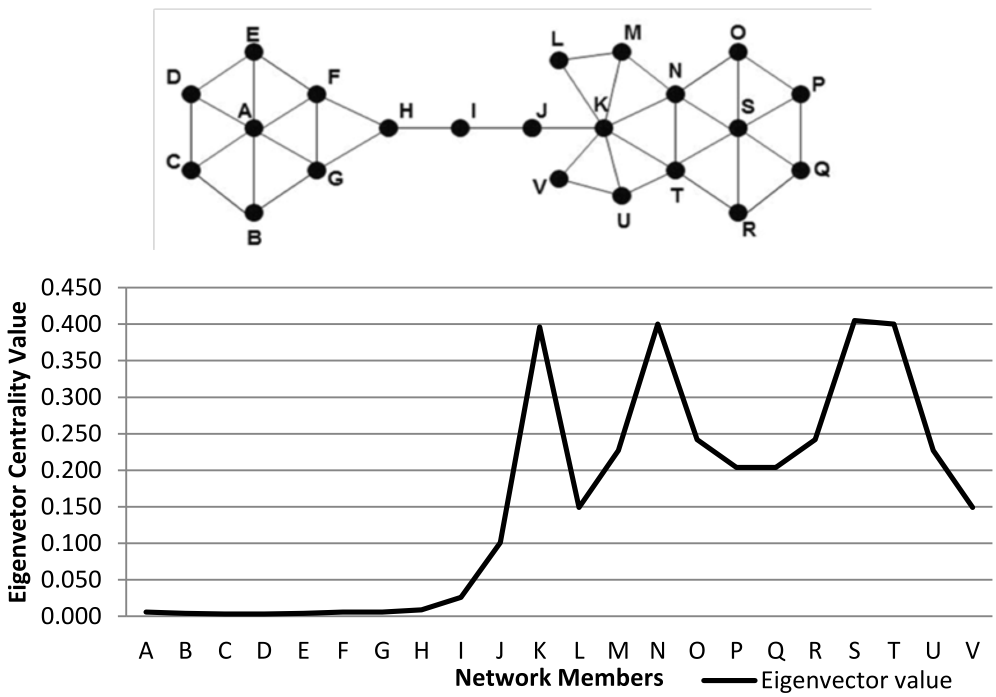

Figure 20. A graph to demonstrate the eigenvector centrality. Actors K, N, S and T are highest in eigenvector centrality because they are directly related to members who have more direct relations, in part, because their end of the network is larger.

* By no accident, these same members rank the highest in UCINET's "Coreness" measurement.

G. DOING SNA: INDIVIDUAL ACTOR MICRO-ANALYSIS

Analysis of individual actors in a network starts with the input data about him or her. An important step beyond the facts and assumptions about types of actor relations, and where SNA helps tremendously, is the associations that stem from those attributes. Relationships with groups of people with like attributes may be indicative of the actor's embeddedness qualities. Said another way, actors of like attributes and relationships with one another may indicate a layer of the subject actor's network neighborhood. For example, relationships with a group of people, who are also interconnected, who all have an affinity for playing poker on a certain night at a certain location belong to a single layer of an actor's network. That same actor will also have relations with a group of people calling themselves by a common family name, constituting a second layer to the actor's network neighborhood. Thus, he is embedded in both social groups. Analyzing a particular actor's range of relationships will likely present evidence of multiple layers of networks—this is the network revelation of embeddedness. When layering the relevant networks over one another, the importance of this actor should become apparent.

1. Ego-network Analysis

In network analysis, true understanding of an individual actor includes understanding his friends, family, co-workers and other associates. This is portrayed graphically in his ego-network, or ego-net. In theory, an actor's ego-net should tell us much about that actor. Among other attributes and relations, an analyst should be able to extrapolate what are the primary sources of information and influence for the target actor, as well as his ability to control or influence others. The attributes of the actors in his ego-net should say something about his beliefs, attitude, and trust patterns. The age or duration of ego-net membership can give insight into some of the processes which require trust and influence such as advice and mobilization to action. An example of an ego-net—actor A's ego-net—extracted from a larger network for analysis is in Figure 21. If the ego-net is very dense, and its members have been friends for many years, and have shared experiences such as school attendance, youth club membership, and all have witnessed the violent death of at least one parent or sibling at the hands of a government agent then the group can be said to be very embedded in many respects. So there are several descriptions that an analyst can derive from the group social processes[167] and constraints under which the actor operates.[168]

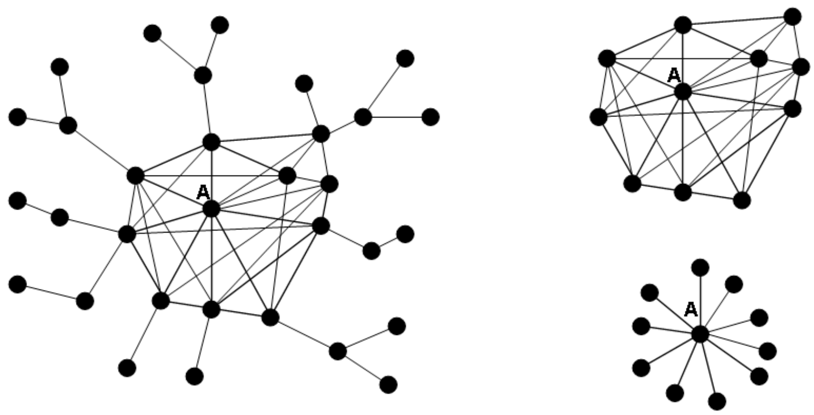

Figure 21. Extraction of an ego-network for analysis. In this instance, actor A's egonet has ten actors, or nodes with whom A has direct ties. The left-most graph is a complete network of A's embedded relations; the top-right is the extracted graph of A's full 1-degree ego-net relations; the lower-right is A's ego-net as a hub-and-spoke graph.

In a world of finite resources and time constraints, the SNA analyst's findings ought to inform the commander's priorities. The priorities concerning which key players to pursue first and subsequently, where to direct further analysis and how to seek maximal positive effect given imposed limitations can be informed by meaningful SNA. The decisions concerning rank-ordering of network members, pathways, and even methods of direct or indirect intervention will combine the information given by centrality measures, network-wide measures such as density or cohesion, and individual member micro-analysis. The changes in structure and roles induced by first, second, and third-order effects of specific acts of intervention—and overall positive and negative effects across the network's neighborhood due to all interventions and environmental impacts -- must be considered.

H. A FINAL WORD ON SNA CONCEPTS AND DARK NETWORKS.

To construct a useful database of network relational information, a solid conceptual and practical grasp of SNA concepts and methods is a must. This conceptual understanding should re-frame a special operations analyst's overall demand for information and imply a change in the practical approach to intelligence analysis. As for the analyst, data entry is merely the beginning of a journey through the process—the end of which is unknown and may provide useful insights into some fundamental questions about the networks, key players and mechanisms in question.

Leading into Chapter V, analysis of a dark network using SNA should enable an analyst to proceed through an informed deliberate assessment process. Any assessment will begin with the fact that a threat group exists and must include enough data about its membership to begin analysis. In an example assessment tree in Figure 22, the first question forces a broad estimate of the target network's functionality and capabilities, and the last completes the assessment with an estimate of intervention tools and resources available for employment. All answers with a "no" or "do not know" response require some combination of further examination of the target network and its neighborhood or assumptions about the network structure to be validated later.

SNA is a very dynamic but still emerging methodology for understanding social networks. At its best, SNA will not be a cure-all for solving the targeting and planning dilemmas when fighting dark networks due to all the vulnerabilities of the fog of war and Sparrow's planning assumptions. However, it provides a methodology for discovery and insight into our human conflict domain previously unseen in intelligence analysis and ought to change the manner in which we demand, collect, compile, analyze and interpret information about dark networks. The ensuing hybrid model of dark network analysis combines the concepts of special operations target analysis and SNA to inform the special operations targeting process.

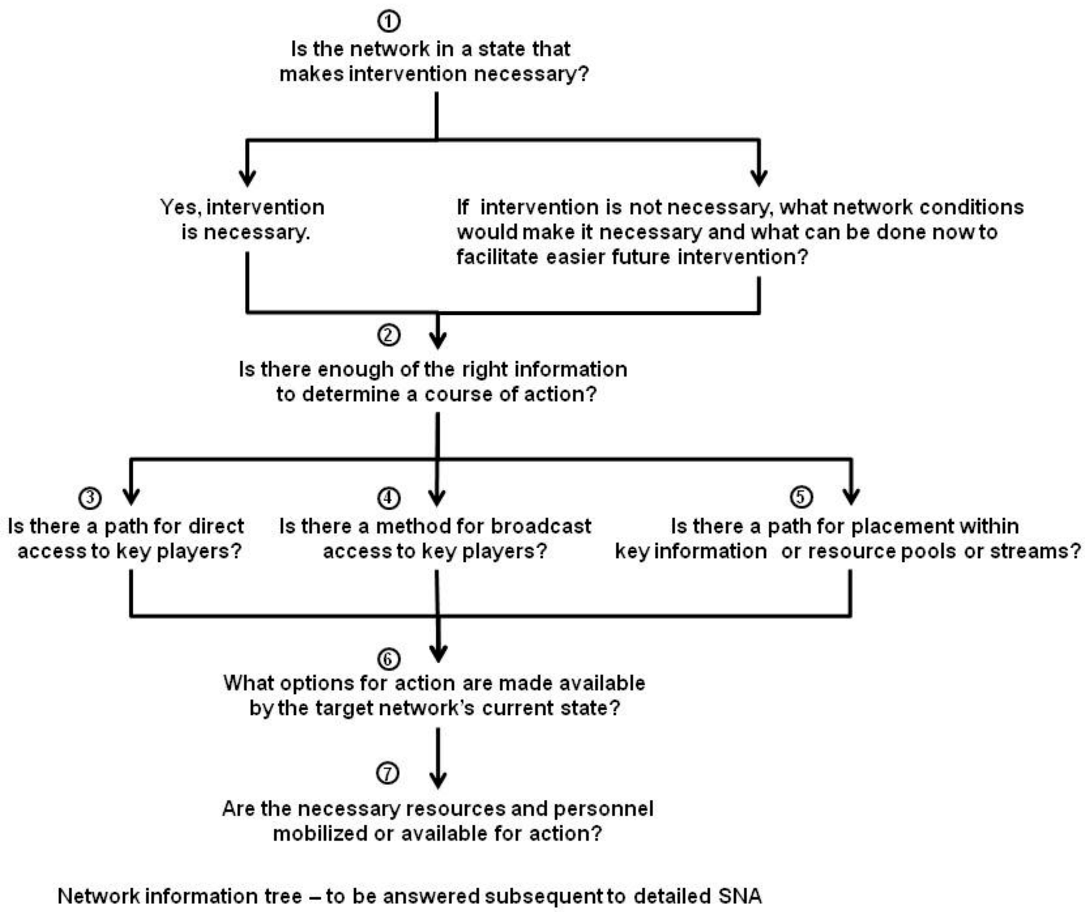

Figure 22. SNA assessment of network state process.

V. THE HYBRID METHOD: SPECIAL OPERATIONS NETWORK ANALYSIS PROCESS

A. STRATEGIC VIEW OF A NEW FRAMEWORK

In wars amongst the people, "understanding the context of [an] operation is as important as understanding the superior commander's intentions."[169] So, when engaging in irregular warfare, the target network's embeddedness in the greater network neighborhood is a significant part of its context[*] and a vital level of analysis.[170] The question of applying the special operations target analysis process to the human domain is that, until now, it lacked a framework for that domain analogous to the one that exists for technical systems. SNA provides that framework. Just as the organizational, technical and physical systems within a hydroelectric dam (see chapter 3) give structure to its analysis, SNA illuminates the structure and relationships of social networks. The idea of applying CARVER as an effects-based approach to an irregular warfare problem is not new,[171] but it has not been applied using SNA concepts and methods. The essence of combining SNA and the special operations target analysis process, then, is matching applicable SNA concepts properly to the CARVER method used in target analysis and evaluation. This method is called the Special Operations Network Analysis Process, or SONAP.

This chapter is focused on the process of SONAP intervention against dark networks. First, it blends the CARVER concepts of target analysis and SNA into an analytical tool, sketching out a typology of intervention concepts, and describing social network-based actions within those intervention concepts. Following the description of SONAP, it expands on the concept of dark network mechanisms and the purposes they serve within a dark network. The chapter concludes with a typology of social reactions to outside intervention.

---

[*] The other parts of a group's context for this thesis are its narrative (its history, present situation and future destiny) and the operative culture that surrounds the group, its origins and its key players.

Briefly reviewing CARVER, we know that it can be used to analyze target systems—target networks—at the strategic, operational, and tactical levels of operations. Again, actions at the tactical level (tactics) are routine procedures used to carry out the orders derived from the operational level plans intended to achieve the desired goals of a chosen strategy meant to eliminate a threat. Networks exist that can be characterized as strategic, operational, and tactical structures, and SNA can assist in understanding the structure of local, regional and national or international relationships that support an enemy's campaign. The CARVER tool enables analysts and planners to disaggregate multiple, interconnected systems to their sub-systems and mechanisms, and describe how they are structured and connected. Combining CARVER and SNA is a method to give a describable and measurable structure to target systems involving social networks.

B. UNIVERSALITY OF THE FRAMEWORK

In keeping with CARVER's applicability to all levels of war, the new model must also be applicable to all levels. Referring to Figure 23, we begin with pairing the three levels of war with three levels of networks as derived from Sydney Tarrow's descriptions of interconnected local/tactical, regional/operational, and international/strategic actors involved in collective action.[172] In this way, social networks may be analyzed at each level of war using CARVER to identify critical systems and sub-systems of social collectives and systems.

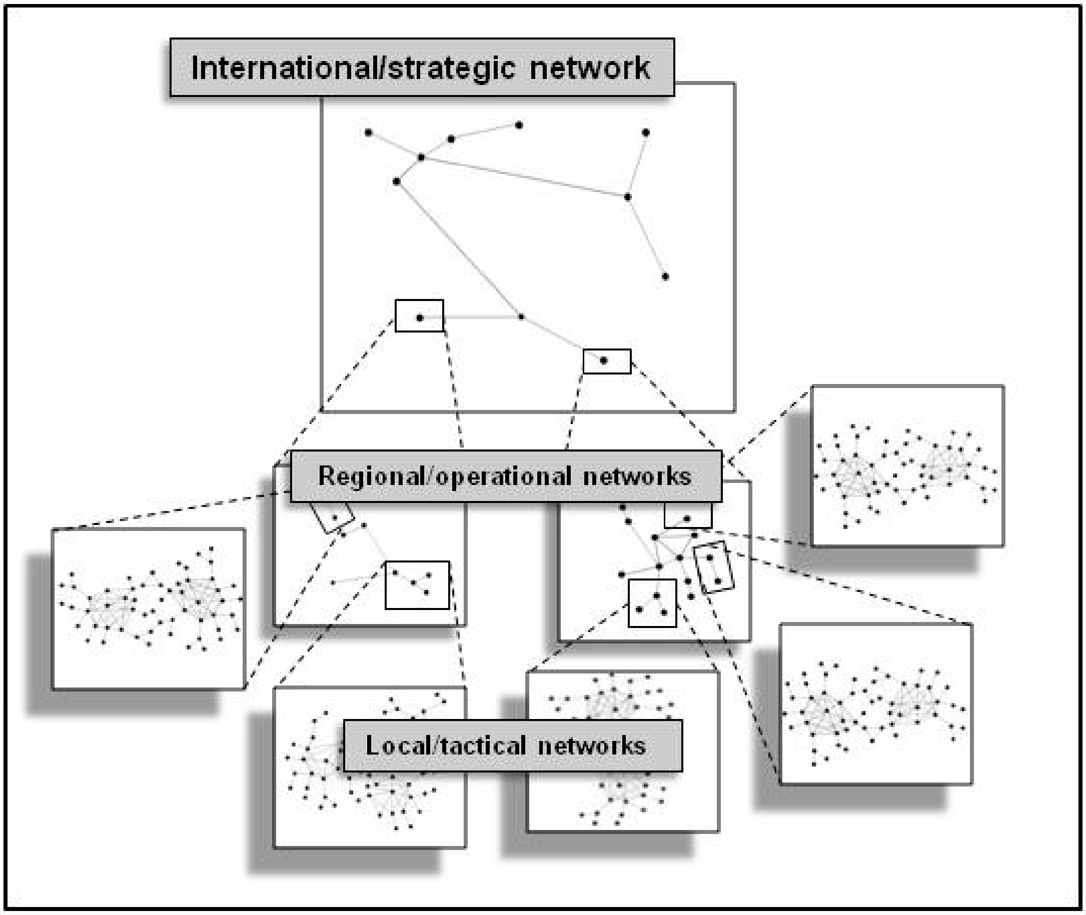

Figure 23. An example portrayal of international-strategic, regional-operational and local-tactical networks. Graphic by the author.

C. COMBINING CARVER AND SNA

Combining CARVER and SNA requires matching like and complimentary concepts. In so doing, there are matches that are conveniently complementary and some pairings that are not readily apparent and require some explanation. Some pairings support more than one CARVER concept. Figure 24 displays these pairings. SNA core concepts are not the only applicable concepts. Kathleen Carley's application of the cognitive load concept is a key consideration when knowledge of network members' intelligence, experience and personality types, such as extraversion and introversion, are known or templated.[173]

CARVER Concepts	SNA Concepts supporting CARVER analysis
Criticality	Individual: Centrality measures, KPP-Pos, KPP-Neg, broker-identification, cognitive load, in-degree, out-degree, structural holes Group: hierarchical clustering, pathway identification, structural holes
Accessibility	Direct access: Supporting pathways (via ego network and embeddedness), geospatial-temporal analysis Broadcast access: geospatial-temporal analysis
Recuperability	Redundancy: structural equivalence and density, ego network, weak ties, structural holes, cognitive load Regeneration: cohesive subgroups + cognitive load, weak ties
Vulnerability	Structural: Structural holes, low number of triads/lack of Simmelian ties, lack of social buffering (few members surrounding core or other critical members) Trust: principal-agent/agency problems through above structural indicators
Effect	Centrality measures, Simmelian ties/triads, embeddedness, strong ties/weak ties, cohesive subgroups, structural equivalence and structural holes
Recognizability	Ego network; geospatial-temporal analysis

Figure 24. Matching CARVER concepts with SNA concepts.

1. Criticality

The pairings begin with the CARVER concept of Criticality. Criticality is the description of the importance of the roles and functions of an individual member, cell, or mechanism to the overall function and operations of the entire network. It must be noted that criticality in SNA is not confined to the traditional military ideas of critical capabilities, resources, and vulnerabilities. SNA concepts that indicate individual member criticality are centered on measures of global centrality, Borgatti’s Key Player Problem KPP-Pos and KPP-Neg measurements, identification of structural holes and brokers, cognitive load and—for directional networks—in-degree and out-degree. At the group level (cells or mechanisms), estimating criticality includes hierarchical clustering, pathway identification (what the military calls link analysis) and understanding the effect of structural holes between groups, or the structural holes in the relationships that embed a targeted sub-group in a larger grouping.

2. Accessibility

Accessibility is a description of the ways and means in which an organization could reach a targeted individual or group. Accessibility is divided into direct and broadcast access. Direct access requires infiltrating or influencing the targeted member’s ego net by point-to-point contact and may consist of physical or electronic contact. The first of two modes in which the Internet plays a role in accessing a targeted member is inherent in direct access via email, chat, messaging, and search function. Broadcast access presumes that the targeted member is not utterly isolated from all outside media by either first-person reception of media signals such as TV, radio or Internet, or that the targeted member's ego net is not also isolated. While traditional radio broadcasts are geospatially anchored, that is that these signals are transmitted from fixed regional or near-by locations, satellite TV and the Internet are not but are still limited in that they both require a baseline level of infrastructure such as electricity, a satellite signal or an Internet Service Provider (ISP), and proper interface hardware and software with proper maintenance and updates. Effective geospatial-temporal analysis will allow analysts to establish a template of regular contacts, locations, and events that will enable synchronizing friendly activities to the enemy's. Establishing action criteria along the lines of accessibility greatly improves chances of proper timing and successful outcomes of friendly actions, or cessation of activities.

3. Recuperability

Recuperability is the capacity to engage lost or diminished capabilities in the form of key players, functional cells, or mechanisms. Recuperability is future-oriented. There are two primary forms of recuperability in SNA terms: redundancy and regeneration. Redundancy, or having an on-hand member, cell, or mechanism that can assume the roles and functions of the lost capability is the more readily apparent of the two forms. These actors or social structures are already present in the network and may be analyzed as long as the analyst includes these structures in his fuzzy boundaries approach to identifying the limits of the network. A danger here is that these structures may not be activated and may be lying dormant while the primary actors are in operation.

If task differentiation and distribution was somewhat evenly distributed according to individual and group capabilities, then other members may be able to assume the missing members' tasks. This is where Carley's cognitive load measure fits in. Network members may be able to assume the roles of lost members as additional duties or change roles altogether and redistribute the task load if it is not too much of a burden for the group. Cognitive load is a very difficult set of attributes to collect against, let alone estimate the relative load-to-capacity ratio per individual and group, but it ought to be a point of analysis of a group redistributing tasks to make up for a lost member or subgroup. Network evidence of a group nearing a 1:1 ratio of load-to-capacity may be a change in the strong-tie structure and in- and out-degree centrality as the new workload consumes more time and energy and different relationships take higher priority.

The other form of recuperability is regeneration. Assuming a reasonable amount of analysis was completed—and the analyst discovered the correct boundaries of the network—regenerative capacity may not be visible. These may be contained in network members' weak tie relationships. Whether a member's weak ties are unique to that member or consist of infrequent contact with the now missing members' strong ties, these relationships are troublesome for analysis. There may be scant or no evidence collected whatsoever that would bring these relationships to an analyst's attention. The only way to assess these relationships could be in hindsight or require a deep dive into network members' histories to see if anything could be estimated as a reach-back option for regenerating a critical lost role or function.

4. Vulnerability

Vulnerability is the two-fold view of network structural and interpersonal trust openings for intervention. On the network structural side, vulnerabilities can be determined by the presence or lack of structural holes within the network and between the network and local environmental actors (i.e.: local resource providers or key social elites) and between the local-tactical network neighborhood and the operational-regional or strategic-international networks, low numbers of triads or Simmelian ties, and a lack of social buffering between core members (with critical roles within vital functions) and the peripheral members. Trust vulnerabilities principally include the universal reliance of leaders upon managers and managers upon soldiers to do the work in the manner and extent expected. Hence, principal-agent problems are likely to be consistent options for exploitation.

5. Effects

Effects are the most difficult to translate from technical systems of the systems world to application in social networks, particularly when trying to predict intentions and future outcomes. This is because effects –reactions—are the most complex reflection of the structure of the network layers and dynamics within each layer and across multiple layers. Effects analysis is also the most reliant upon knowledge of key members' cognition and awareness–something nearly impossible to guess and may require an extraordinary effort to establish a working knowledge. Key indicators of how effects will flow across a network will be measures of centrality, quantity of triads (especially highly central members of Simmelian triads with other key members), strong ties/weak ties, cohesive subgroups (especially cliques), structural equivalence, and structural holes. Analysis of the effects component may be partly informed by analysis from the Criticality and Recuperability components (as in, once a critical node is removed, the first best option for replacing that node will be activated and employed, thus possibly shedding that member's previous task load onto one or more other nodes).

6. Recognizability

As the last component of CARVER, recognizability may be the simplest to bridge from SNA. Recognizability refers to the ability of outside analysis to detect and identify specific members, cells or mechanisms. Traditionally, this meant readily identifiable physical appearance. In SNA terms, recognizability is the sum of key indicators of physical presence, communication patterns, intentions, known direct relationships, and actor-unique attributes or artifacts. Specific aspects of SNA that support recognizing someone by those indicators are ego network and geospatial-temporal analysis. When physical recognition is not possible, then identification of the pattern of others' actions each time that member is in proximity will be the alternative recognition.[*] Target members' ego networks may behave in certain ways when the member they are around, and perhaps differently when they are not. When a certain subgroup changes actions in a

[*] See the description of information triangulation in the first chapter.

certain way whenever a neighboring subgroup is active, then analysts may establish that as a pattern and build plans for action based on that activity.

D. THE TYRANNY OF THE STRUCTURAL HOLE

The reader may notice the prevalence of structural holes in Figure 24. The significance of structural holes in the market economy of irregular conflicts cannot be overstated. Insurgent, social movement, and terrorist networks live or die by their ability to reach desired resources, enemy assets, target audiences and recruitment populations, all while retaining some level of secrecy. In the case of terrorist and insurgent networks, the level of secrecy required for survival and the costs of resources and time expended to maintain it can be extremely high.[174] Those who cannot maintain it die or are imprisoned. For the members who survive and endure, the buffer that members build between themselves and those around them who are not part of the movement or group are real or effective structural holes. In a very real sense, good secrecy is a blanket of structural holes that is tightly controlled and monitored. So, the purposeful structural hole is not just a physical dimension of secrecy, but it is a cognitive one as well. And not just for secrecy or access and placement for intelligence collection. Breaching or brokering across a structural hole can be a basis for action, a motivation to mobilize recruits and resources, to broadcast ideas to the target audience. Enter the war of ideas.[175]

Ideologies are structured ideas with larger meaning. Ideas, and identities derived from them, are best adopted under the influence of a narrative, or story, which makes a point and connects the dots for an audience, partly as a tool for mobilization.[176] Dissemination of political and social narratives is subject to the power of structural holes such as a group's description of its history, its critical role in society and its destiny must be able to reach the desired audiences in palatable and believable ways in order to propagate and mobilize recruits and resources. The physical dimension of idea dissemination is one actor in proximity to another other, several or many actors via broadcast media; someone must do the reaching out Within the realm of ideas, frame bridging and alignment are necessary to co-opt a target group's narrative and demonstrate aligned grievances and destinies.[177] These serve to inform or prescribe social or political change and then motivate target audiences to action.[178] The cognitive bridging process exists because there are cognitive structural holes in the network of ideas and motivations. If there is no transmission method or agent capable of reaching the intended target audience, then a structural hole exists between the group and the target population, and the group may wither and die or be condemned to isolation.

E. INTERVENTION METHODS AND APPROACHES

1. Typologies of Intervention

The typology of intervention methods is comprised of four levels of targeting, four methods of action, and three time-based approaches to intervention. The four levels of targeting are: individual nodes or members, cells, mechanisms and networks. The four methods of action are: monitor, influence, replace, and eliminate. The three time-based approaches to intervention are: individual, segmental, and sequential-viral. This typology is intended to give structure and relations to the key aspects of targeting such that the manner of intelligence collection against dark networks is fully informative and supportive of campaigns and operations.

The purpose of targeting is to induce responses that change network structure or operational imperatives, or both. As noted earlier, these responses take the form of a hierarchy of effects: first, second, and third order effects. In wars amongst the people, the first order effect is cognitive, the second is communicative, and the third is physical or structural. It is this pattern that ripples across a network, causing choices to be made and communicated at every level impacted by the causal event. With this in mind, the actual form and manner of the interventions applied against a network must be carefully created according to the best information available concerning the network structure as it stands, and how these effects can be transmitted and interpreted. The actual interpretations by the network leadership will drive their preferences and, according to the relational and cognitive structure of the decision making body, lead to decisions about network structure and operations.

The levels of targeting are in order of increasing scale of network formation: individual member, cell, mechanism, and network. Individual members or nodes are the most basic building block of a network, and knowing their roles in dyads, triads and larger network formations are critical to understanding the financial, social, psychological and political capital investment into an endeavor.

Cells are cohesive subgroups that are or approach all-channel cliques that have a collective purpose, based on the capabilities and capacities possessed by the cell members, and have one or very few direct relationships to outside actors. In network terms, cells are nearly surrounded by structural holes. Cells can be deliberate or natural social formations, but their internal dynamics are characterized by strong ties. That is, the members have frequent and meaningful internal communications and other exchanges. Members of a cell are very close and depend upon each other for many aspects of daily life, especially in a violent conflict environment. They trust each other in very important ways. A cell is a form of purposeful, cohesive subgroup very much like an all-channel clique, with one or very few connections to the rest of the mechanism or network in which it is embedded.

2. Network Mechanisms

Mechanisms are social networks with deliberate routines–sequences of exchanges and systemic processes–that require contributions above the individual level and deliver information, services, or resources from an outside source to the interior or functional membership of a larger network. A mechanism is a chain or larger group of nodes or cells with a unique capability which it regularly executes. An example is a supply chain, or logistics mechanism, that reaches from deep within the core of a network to the outside world where the resources it acquires originate. Properly governed mechanisms also differ from cells or other cohesive subgroups in that there are structural measures employed throughout a mechanism to maintain a balance between synchronization and security, as well as control and efficiency.

Mechanisms also respond to demand signals at the parent network end, are dependent upon both the larger network at the demand end and their external sources at the supply end, and must negotiate for fair exchanges at both ends. Mechanisms may be considered networks in their own right, depending upon the level of analysis being conducted, and embedded in their surrounding network neighborhood by deliberate representation at key points. Mechanisms include multiple members and cells that are linked together but with structural holes built into the formations, either naturally-occurring or deliberately. However, mechanisms are not all-channel networks with consistent Simmelian ties to ensure member compliance or agreement, and thus are also constructed with inherent vulnerabilities. Mechanisms will be discussed more in the following sections.

The highest level of intervention is the network level. While networks are the largest social formation in social network theory, and some network theorists extend the network concept to the entire world.[179] For purposes here, it suffices to say that networks are embedded within larger networks and merge together via shared membership. For future references within this thesis, the network is the highest level of analysis and consists of nodes, cells, and mechanisms.

3. Intervention Methods

Next, there are the four methods of intervention. All actions are contained within these four methods ranging from least to most intrusive: *monitor*, *influence*, *eliminate* and *replace*. The level of sophistication required to accomplish these methods varies according to the scale and sophistication of the security surrounding targeted network. A decision to *monitor* a node or portion of a network drives resources and planning to observe and collect any and all information concerning actions, intentions, plans, resources, capabilities and limitations of the targeted node or nodes. As it is the least intrusive method, monitoring a node may be most desirable and frequently applied. The is especially true when the node is a key player for information awareness in a network or part of a decision-making or critical asset delivery mechanism. It may provide some level of early warning of impending attacks or other intentions.

Influencing a node offers a very wide range of options, from direct to indirect messaging or physical actions against members of the targeted node's network neighborhood that could reliably cause the node to change behavior. All forms of communication and actions are available, depending on environmental constraints such as rules of engagement, international law, native development and technology, local culture, and local laws and customs.

Eliminating a node is the easiest to explain. Th is is action to kill, capture, or otherwise remove a member from this network neighborhood. The effects of this removal may be partly informed by Borgatti's Key Player measurements, but the analysis beforehand ought to include the best estimates of who would replace the member to ensure the role or roles he played continue to benefit the network.

Replacing a node is by far the most difficult and forces a group to assume the most risk. Replacement is taking the role and position of a targeted node in the network. Elimination is inherent, but must be conducted in a manner that allows for a specially designated and trained element to be accepted by the targeted network and operate in the missing node's place. In trust-based dark networks, this is challenging to say the least. Yet, there are historical precedents for it that will be discussed in Chapter 6. Organizations implementing these methods do so by determining the scale of the intervention, or choosing an intervention approach.

4. Intervention Approaches

The three approaches to intervention are based on the number of network members to be acted upon and the timing of those actions per iteration. The approaches are *individual*, *segmental*, and *sequential-viral* and are listed in increasing level of requisite synchronicity and risk to the desired outcome. The choice concerning type of intervention is informed by:

1. The desired outcomes as articulated in the commander's intent
2. The amount of risk the command is willing to accept
3. The demonstrated level of organizational flexibility and agility
4. The assets and resources available and the ability to direct and synchronize them

The chosen approach drives the sophistication and scale of intelligence collection, analysis, and operational planning, as well as understanding any associated contingencies. The i*ndividual* approach means taking action to remove a single member from active participation in his role in the larger network functions. This type is the least intensive for intelligence collection, analysis and planning purposes. The *segmental* approach refers to taking action against a definable or bounded part of a network simultaneously, whether that segment is a cell, an entire mechanism, a range of brokers that connect components of the network, key leadership members, or some other subset of the network. It requires a higher degree of synchronization than the individual approach to ensure that none of the intended members from the target set escape.

The *sequential-viral*[180] approach is a planned multi-iteration version of one or both of the other two approaches. This is a much more sophisticated approach than a single-iteration in that it requires organizational flexibility and agility in decision making, execution synchronicity, and contingency planning. There is a higher degree of risk because there is a greater chance of the later-targeted actors being alerted to their cohorts' detention.

5. Intervention Concept

An intervention plan—actually an *intervention concept*—would include all three components: a level of targeting, an action type, and an approach. An example concept is: *we will conduct a segmental elimination of all members of cell A, simultaneously with replacing their courier (individual member replacement) to the regional command cell with a recruited agent*. One possible intended outcome from this operation is that an entire intelligence collection cell is arrested, plus their courier who delivers their written reports and other messages is arrested and replaced by an agent who can facilitate deception of the regional command cell by delivering false intelligence reports. Amplifying information such as monitoring the command cell to ensure they are unaware of the operation may also be included. If this operation is nested within a larger operation to influence the regional command cell by deception, then the concept would state so. Describing an intervention concept like this is intended to impart a basic understanding of the actions involved, against whom, and how it is to be carried out. The details of each intervention will be exhaustively described in the plan that follows from the concept, with the purpose of each action and how it connects to the larger purpose of the operation. The range of possible effects of a successful—and unsuccessful—mission outcome should also be described, based on the network analysis.[*]

---

[*] Currently, military doctrine only mandates description of the effects of a "most likely" and a "most dangerous" outcome. Complexity demands admission of the possibility of a range of possible outcomes according to the effects associated with any operation.

While at first glance some permutations of the above would seem simpler than others, the best choice for any given situation lies in the quality of the data, the quality of the analysis of that data, and the soundness of the plan derived from that analysis. For example, eliminating an entire network that employs no security measures and is entirely mapped out and predictable from their routine activities may be far easier than replacing a critical node with a friendly agent within a family-based mechanism funneling weapons between trusted tribal areas. Thus, the former option may be a matter of timing more than complexity. In the case of the latter, the opacity and cohesion based on trust of the targeted node's network neighborhood is much more of a factor. In this way, intervention difficulty can be a function of the locations of structural holes between the acting organization and target network. So, a solid understanding of the structures within a dark network is necessary to determine the best options for intervention.

F. MECHANISMS AND THEIR FUNCTIONS

Mechanisms are specialized chains and groups of members that collectively accomplish a unique task or set of tasks routinely. Each member has a specific role or roles that he or she performs for the surrounding network neighborhood, such as leader, driver, foot soldier, courier, or bomb emplacer. Individual members may form cells as needed to accomplish more involved tasks. Or cells may become part of a dark network as a legacy structure borrowed from another social network, such as familial ties or other social groupings; the sources of recruits vary greatly. Mechanisms may also form either from an amalgamation of individuals or cells for specific purposes or from an intact system such as a legitimate private business turned into a front organization. Regardless, the social groupings known as cells and mechanisms have particular functions to perform with at least a minimal level of competence. As a *role* is to a network *member*, so a *function* is to a *cell* or *mechanism* within that network, so that *functions* are the tasks that mechanisms accomplish for the larger network. Depending on their size, purpose and environment, dark networks have seven basic functions that must be accomplished in order to survive.

The seven sufficient and necessary functions of clandestine networks are 1) leadership and decision making, 2) ideology and messaging, 3) operations, 4), intelligence 5), resourcing (acquisition, logistics, storage, and financing), 6) sanctuary, and 7) recruitment and training. If a particular dark network has a more specialized function overall, then other, more focused and specialized mechanisms may appear as subsets of the above list. It is also important to note that, as networks grow and take on larger memberships and seek to achieve greater objectives toward their overall goal, they go through processes of specialization and differentiation. Mechanisms may subdivide and the new departments focus their work to fulfill larger functions[181] based on the uniqueness of tasks, technical difficulty of processes, geographic distribution, and the need for secrecy.[182] There may be multiple examples of one kind of mechanism contained in or supporting a single operational network due to the above factors.

Dark network mechanisms and their functions are interdependent, with some more central than others. Figure 25 shows the interconnected functions, with leadership & decision making, ideology, operations, and intelligence as the most central functions.[183] The relations between the functions are only part of the story, however. The lines are connections between members, just as the cells and mechanisms that perform the functions are made of connected members. The various mechanisms attempt to synchronize functions with each other so that the collective may achieve some level of success.

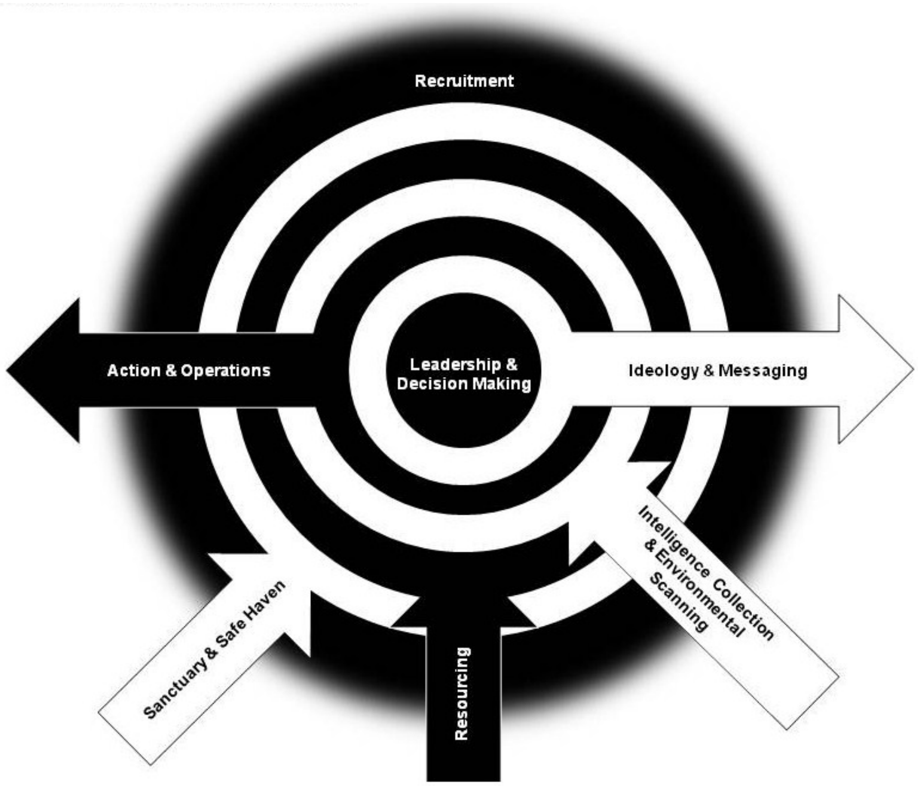

Figure 25. Dark network functions. Each outer function supports the inner functions structurally and conceptually. Graphic by the author.

G. ESTIMATED NETWORK REACTIONS TO INTERVENTION

Mechanisms embedded within networks are networks themselves. The members of a mechanism send and receive signals from their network neighborhood just as any other social network. What has not been discussed in sufficient detail, however, is a typology of the full range of responses available to a dark network to stimuli from the network neighborhood. Knowing the range of possible reactions provides a bounded set of effects that may be deduced and understood in terms of structure, centrality, cohesion, density, and other SNA concepts. Since dark networks will not behave in random ways when they detect intrusion or come under attack, their reactions can, theoretically, be predicted. They will behave within a bounded set of estimated* reactions. This is important because *predictive analysis* is critical to understanding the first, second, and

* The bounded set of reactions is only an estimate because of the three fundamental planning assumptions of dark network analysis (see chapter 4).

third order effects of network intervention, and what is needed to move the network in a favorable direction or at least see what you may have to deal with after intervention. The military's current model of action-reaction-counteraction will suffice for a simple method of examining effects based on initial friendly force intervention.[184]

Intervening against a dark network can have two primary effects on the network: structural and cognitive. A dark network's reactions to external attack, or suspicion thereof, will have different effects on the membership depending on the intervention (level, method, and approach), network cohesiveness, and the countermeasures taken by the network as a whole or by significant portions of it. The actions of a member's immediate network neighborhood will significantly impact that member's sentiments and actions.[185] Not only may the network's structure of relationships change (structural changes), but the quality of those relationships and sentiments may change (cognitive changes). Thus, not only the intervention, but the reaction and counteractions will have both structural and cognitive effects on the network. The goal of intervention is to maximize the negative impact of both types of effect. The goal of the target network is to limit the structural and cognitive damage caused by intervention and reduce risk of further compromise by making structural changes that improve security and effectiveness that also maximize favorable cognitive impact.

1. Structural Reactions to Intervention

Structural effects are changes to the membership and relationships between members. The cognitive effects are characterized by *favorable* or *unfavorable* impacts on members' levels of trust, perceptions of uncertainty, and morale. Unfavorable cognitive impacts include decreased trust with current or new local network neighborhood members, increased perception of uncertainty and lowered morale.

Initial conditions are very important to the quantitative and qualitative evaluation of changes and patterns across the network under analysis. These conditions refer to circumstances both internal and external to the network at the earliest time of discovery. Obviously, this is problematic when discussing dark networks, and the information available at the time of intervention will have to suffice for initial conditions in order to measure changes due to intervention. The internal conditions include as many of the qualities of social networks as may be measured: strengths of ties, centrality, density, positions and roles, size and relations of cohesive subgroups, and number of triads. Bridging the internal and external are the relationships that connect the network to its network environment. External conditions include environmental factors such as similarity of the dark network to the local (open) population, homogeneity of the local population, availability of resources to the network for exploitation, technological development of the surrounding region, and the popular legitimacy and skill of the local authorities to influence relevant segments of the population.

Two further assumptions are necessary to explore theoretical network effects. First, the network is assumed to correctly perceive and disseminate internally the intended signals from the outside by the individual senders, including an intervening organization. This will attempt to hold constant cognitive and organizational biases and other filters that screen out important information, except for when creating these problems is part of the intended outcomes of an intervention. The second assumption is that all network members are action-oriented, as indicated by their membership, and pressure their leadership to continue action via their routine interactions. This assumption attempts to eliminate membership apathy or disenfranchisement for reasons other than the effects of intervention. However, these factors cannot be held constant in real life unless the network locations of these conditions are known to exist and the planned intervention is intended to exploit those very dynamics already at work.

The structural impacts are categorized by *consolidating* effects and *dispersing* effects, which are decisions or actions to expand or contract the direct control or influence of the core of the network relative to the size of the network and scope of operations. In other words, the network core is consolidating power if they take actions to expand direct control by either shrinking pathways to desired nodes outside the core or by exerting dramatic constraints over the conduct of operations. Conversely, the core disperses power structurally by allowing the network to expand without shortening network pathway distances to key members or by deliberately increasing pathway distances through some form of reorganization. Operationally, the core disperses power by allowing subordinates autonomy of action through independent decision making and resource control.

2. Cognitive Reactions to Intervention

The ability to influence the core of a network to change structure of functional norms is dependent upon the network's ability to correctly perceive outside signals and communicate internally. Cognitive impacts are valued as to the benefit or hazard to the mission created by the psychological and emotional impact of a structural change upon the affected members. These effects will impact the individual level as members' stress levels, trust, and productivity are influenced by their network neighborhood. These impacts also apply at the group level as members change their relationships and the quantity and quality of their interactions—thus altering the flow of information, capital, and resources across mechanisms within the larger network. Cognitive reactions to structural changes will be according to known and unknown numerous and likely contradictory factors influencing the opinions and habits of the membership. It should also be noted that repeated abuse, misuse, or misinterpretation of signals across the network can create negative outcomes of any of the structural reactions, even if they are done with the best intentions of the network core or middle-management. So, while predictions are approximations at best (and wild guesses most likely), the cumulative impact of total cognitive effects on structural change needs to be accounted for or assumed to be constant according to a useful framework that helps guide analysis and planning. Figure 26 is an experimental framework in that direction.

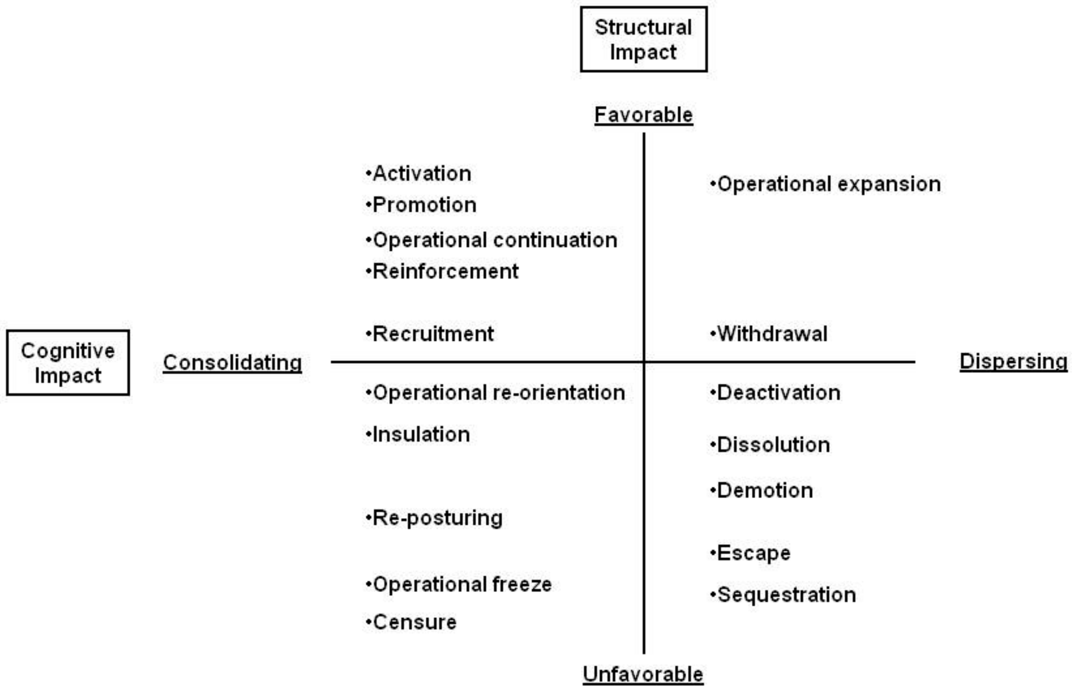

Figure 26. Network status reactions to external stimuli distributed across scales of structural and cognitive effects. Generally, the goal of intervention is to maximize the unfavorable impacts according to how the intervening organization wants to terminate the end game against the network.

3. Consolidating Effects

Consolidating effects increase the level of direct control of the network by bringing members closer together, limiting exposure to external influence, reducing or re-orienting operations, shedding the more peripheral members, or increasing active membership by recruitment to active mechanisms already under direct control. Consolidation also brings additional stresses of increased numbers of direct reports with all the burdens of responsibility for more members and their actions. Indeed, while all structural effects may possess some degree of positivity and negativity, they are valued here according to the likely dominant attribute.

Consolidating structural reactions include *activation*, *promotion*, *reinforcement*, *recruitment*, *insulation*, *re-posturing, and censure*. Also included is a deliberate decision to continue operations called *operational continuation*. The first four reactions have mostly positive cognitive effects as they are in-line with the members' need for action while the remaining three denote mostly negative cognitive impact.

Activation occurs when inactive members of the network are re-structured into the remainder of cells and mechanisms currently functioning, or re-introduced as a newly formed cell or mechanism. Activation is performed according to a plan developed prior to de-activation. Agents who are technically members of the network, but are inactive, are often referred to as "sleeper agents" or members of "sleeper cells."

Promotion is when an active member or members are elevated in status over their peers and perhaps re-assigned to lead a different group of members. Structurally, this is a consolidating effect because the elevated position means they are closer to the core, if not now a member of it.

Reinforcement is re-aligning the network structures accompanying specific functions (members, cells or mechanisms) to support another similar or related function to ensure success of the latter. This is a consolidating effect because these supporting structures are now under the direct control of a primary effort of the network.

Recruitment is mobilizing new members or co-opting other organizations into the network's greater span of control. Recruitment can also have a dispersing effect if the new members are given a high level of autonomy in resource control and decision making.

Insulation is individual members reducing their contact with the outside world (building structural holes) and requires widespread action to merely protect the network, rather than fulfilling the purpose of the network, which forces members to decide to sever non-essential ties to non-members. A severe form of insulation may be a deliberate process of going underground or severing all non-network ties (even with family), similar to the process that members of the Weather Underground underwent when they split from the Students for a Democratic Society organization in 1969.[186] This form of insulation can be resource-intensive and expensive.

Re-posturing is significant restructuring of roles, positions, and joining structures between members, cells and mechanisms and likely includes severing long-standing strong ties, and forcing subordination of members to others between whom there is not a consistent level of trust. In the same light as an adhocracy, destructive change can be very emotionally destabilizing and creates enormous challenges for moral cohesion, trust or continuation of social norms within the group.

Censure includes all forms of punishments (except for demotion) where the member being punished remains under the control and employment of the network.

In network analysis measurements of consolidating actions, some combination of the following may occur: the network increases in size; the average individual member "reach" (centrality measures) increases; the number of extra-network strong ties decreases, while the number of weakening ties increases; the number of structural holes protecting the network increases (inversely with the number of direct connections to external resources and information sources) the number of pairs and triads increases; the number of components decreases; and density increases.

The idea of forcing changes in networks is to create improvements or degradation of CARVER characteristics such as reduced criticality via redundant communications, reduced vulnerability due to the conforming impact of new Simmelian ties, improved recuperability (via increased instances of structural equivalence) and insulation leading to reduced vulnerability. Some structural changes will benefit some aspects of the network's purpose. Others may cause the network to suffer, such as increased vulnerability due to fewer structural holes between cells and mechanisms (less compartmentation) and could lead to compromise of sensitive information and leaks to the outside world. In this way, individual changes could have both positive and negative impact, perhaps simultaneously.

4. Dispersing Effects

Dispersing effects occur when the core of a network seeks to relieve itself of the stresses of managing a network by relinquishing varying levels of control over some or all subordinate mechanisms. This may occur for several reasons: the network may have grown too large and unwieldy for centralized control, because of a sudden change of environmental pressures, because network leadership senses a loss of purpose, or in response to a suspected security compromise. Structural reactions with dispersing effects include *withdrawal*, *deactivation*, *dissolution*, *demotion*, *escape*, and *sequestration*. Of these, only *withdrawal* has the potential of carrying affirming emotion as it indicates a pre-planned scheme of physical removal of network members from one geographical area to another with the intent of resuming operations upon re-establishment in the new area.

The remaining reactions have some level of negative connotation because they are understood to mean separation from the action, trust, satisfaction and assurances of the main body of the network with increasing levels of duress.

Deactivation means a portion of the network is to be shut down for an unknown duration, with a re-activation plan known and rehearsed, and likely without duress other than the necessity for secrecy.

Dissolution is deactivation of an entire mechanism or the network as a whole without re-activation planning; duress level is undetermined.

Demotion is an individual condition of losing status in the network but remaining active, though a group may feel the consequences along with the demoted member (such as a cell feeling an emotional blow due to their leader's demotion).

Escape is to depart a geographical region under severe duress. The physical displacement may be according to an escape or "bug out" plan, but entails some level of a loss of direct control and communication. The network as a whole may not be likely to re-convene intact due to the loss of some or many members in the process of escaping. Withdrawal is a more controlled form of departure.

Sequestration is a protective measure taken by the majority of a network to insulate itself from a smaller component of the network under duress based entirely on the perception of security compromise or a schism of ideology or other form of divisive competition. This may be a temporary or permanent condition, to be determined by the network core. A sequestered portion of a network can be re-validated by a series of tests, pursuant to an investigation, or by re-claiming allegiances depending upon the nature of the crisis that led to sequestration in the first place.

5. Operational Changes

Changes in the conduct of operations–what the network is supposed to be doing–are considered structural because the actions of the members, cells and mechanisms are the structure in motion. In a dynamic environment, static information is nearly irrelevant, as are unused materials, funds, and people. While maintaining a reserve is important for buffering the peaks and valleys in availability of resources or other environmental constraints, the purpose of the network is presumed to be change, radical change. Change requires action.

Changes in activity between members are changes in the structure and flow of the network. These mechanics include employment of trust—the flow of social capital—and the flow of information and resources. In total, there are four choices of operational directive available to network leaders: *continuation*, *re-orientation*, *expansion*, and *freeze*.[*] *Operational continuation* is to maintain the status quo—members keep doing what members desire to do by virtue of their decision to become members in accordance with leadership decisions and resource availability. *Operational expansion* is to multiply the members, cells and mechanisms dedicated to certain operations by re-arranging membership or improving efficiencies in structural distribution or resources. However, *operational re-orientation* and *operational freezes* have negative cognitive association because they pull members off their patterns of normal operations, thus increasing stress and perhaps diminishing trust between themselves and their superiors. This is especially acute in *operational freezes* as members sit idle, and perhaps go off in search of meaningful work with other illicit groups, or even seek employed in the open market and leave their previous dark network associations for good.

In a final word about structural change options, consolidating and dispersing effects that look the same structurally can be for offensive or defensive purposes. For an offensive example, a network may prepare for expanding operations by splitting a mechanism into two separate mechanisms with unique command and control structures (i.e.: creating two separate attack cells by either time, or space, or both.). Or, defensively, network leadership may split a mechanism in order to sequester only a portion of it due to inefficiencies, ideological disagreements or suspected security compromises in order to preserve the remaining network. In the event of a structural change without much other

[*] Initiation is also an operational choice, but this presumes no action precedes the analysis. This thesis assumes a targeted network is already functions, as that is what brought the network to our attention.

indication of the purpose, observers will have to look elsewhere across the network for corroborating indictors of intentions.

H. SUMMARY

SONAP uses concepts common to the Special Forces target analysis CARVER tool and SNA to identify and estimate structural patterns and changes in dark networks. The template used to estimate a basic structure includes seven mechanisms that range from the very core decision making structures to the outer-most recruitment and resource mobilization structures. The six aspects of CARVER have commonalities with SNA concepts as well as other, related concepts such as geospatial, temporal and cognitive characteristics used in other approaches to disrupting dark networks. SONAP also prescribes four methods of intervention, with three intervention approaches to affect changes in network structure and operations. Those changes are measured according to consolidating or dispersing structural changes and positive or negative cognitive effects upon network membership. Naturally, the goal of intervention against a dark network will include maximizing disruption to internal processes by influencing it to make structural and operational changes that reduce operational synchronization and maximize negative cognitive impact. To explore an example of implementing SONAP against a target network, Chapter VI is comprised of strategy development and intervention against Noordin Mohammed Top's Islamic terror network in Indonesia, based on a 2006 open-source dataset.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. ATTACKING NOORDIN'S NETWORK: APPLYING SONAP

A. INTRODUCTION AND BACKGROUND OF THE DATASET

What follows is an example application of SONAP-based analysis and intervention strategy of an open-source dataset from International Crisis Group, "an independent, non-profit, non-governmental organisation [sic]"[187] that produces reports concerning various crisis areas around the world. The dataset is one that describes some members and relationships that constituted Noordin Mohammed Top's hybrid Jema'at Islamiyah terror network that attacked high-profile Western civilian targets in Jakarta and Bali from 2002–2005. Those attacks killed hundreds and caused severe damage not just to the intended targets that included hundreds of Westerners and other club-goers at hotels and nightclubs, but also to the credibility of the Indonesian authorities.[188] The availability of these data and the public record of Indonesian law enforcement and military operations against this network provide an accessible discussion concerning the ends, ways and means of intervening against dark networks. This chapter is a discussion of strategy, desirable and attainable end states, and the work within SONAP that goes into operationalizing the strategy to achieve success. This chapter concludes with one possible strategy to move toward solving the two essential problems the Indonesian government faces in this particular case study. Those problems are substantial gaps in security sector effectiveness and Noordin Top's violent jihadist terror organization operating and conducting attacks within its sovereign territory.

B. INITIAL STRATEGIC CHOICES

Intervening against dark networks requires a fundamental choice of which overall strategy or strategies will be employed against the systems which the network exploits or controls. One of those strategic choices includes decisions as to whether or not to employ kinetic methods, non-kinetic methods or a combination of the two.[189] Top factors influencing this choice are international laws and treaties, host nation laws, U.S. laws governing the authorities granted by relevant policies, and the practicalities of ends, ways and means in military operations.* Diplomatically speaking, it may be in the United States' best interest to abide by existing laws or agreements with the larger community of nations, even at the expense of short term tactical successes or operational simplicity, unless specific laws or exceptions can be granted by host nations† or supportive third country leadership.[190] But the host nation may be unable or unwilling to intervene or to allow others to intervene within its borders. The host nation may even be more or less compliant with the dark networks contained within its borders. Thus, from a theoretical perspective, all options are on the table. Figure 27 displays the range of options available supportive of both sides of that decision.

	Kinetic				Non-Kinetic				
Strategy	Targeting		Capacity Building		Institution Building	PsyOp	Information Operations	Rehabilitate/ Reintegrate	Monitor
Options	US Unilateral, Host Nation, or Combined	Non-Attributable Third Party	Host Nation	Third Party	Host Nation & Indigenous Civil Society	Host nation & non-attributable third party		Host Nation & Civil Society	All-source
Levels	Individual, Group and Institutional				Individual, Group and Institutional				

Figure 27. The range of strategic options supportive of kinetic and non-kinetic approaches adapted from work by Roberts and Everton[191] and Everton.[192]

Kinetic methods include missions intended to result in death or capture of targeted network members, typically known as "kill or capture" missions, or destruction of materials, equipment or facilities. The desired outcomes from kinetic operations tend to be immediate, with second and third order consequences of less direct interest. Kinetic operations can be executed unilaterally or by/with a host nation or third party agency under U.S. direction. There are numerous factors that impact those decisions and the overall effort may require a combination of several of the above options to meet the requirements of the United States, the host nation and concerned third parties.

* The environmental constraints of some locations may prohibit one or more methods, or any overt operating of any kind, thus forcing decisions to be made regarding risk of compromise and its impact upon perceptions of U.S. legitimacy and risk of violations of the terms of international alliances.

† Here, host nations are the countries in which the targeted dark network resides.

Kinetic targeting is only part of the overall kinetic story. The other part is creating or developing the capacity of the local law enforcement apparatus or counter-terror or counterinsurgent military or paramilitary units resident in the government most responsible for the dark network problem. All these entities will be referred to as the host nation's security apparatus. In the case of a willing but incompetent host nation security apparatus, the U.S. may choose to undertake an extensive program to improve the capabilities of a host nation's security forces, domestic intelligence agencies and judicial system.[193] Even then, a foreign nation may still require more direct assistance. However, if the host nation proves unwilling to intervene against a resident dark network enemy, then a willing third party–an irregular force–may be an acceptable option to attack the targeted dark network.[194] This third party may belong to another nation's security forces, or constitute an altogether non-attributable, irregular force not adhering to any nation's foreign policy or security apparatus. This same third party may also demonstrate a limited capability to carry out its intentions, and so may also require some level of capacity building from the U.S. or another party. However, in terms of international norms and laws, the concept of developing and applying a non-attributable third party to this kind of work is a troublesome choice, fraught with potentially damaging blowback.

Aside from kinetic operations, there is another path. Non-kinetic methods include institution building, psychological operations, information operations, rehabilitation and reintegration, and intelligence monitoring. These range from military or military-like capabilities to domestic intelligence collection and operations to decidedly non-military agencies and international institutions collaborating in host nation domestic civil society development. In some cases, an improved range of host nation and indigenous institutions has been able to blunt the extremist ideologies and offer alternative messages to vulnerable audiences and pools of available recruits.[195]

To explain, institution building is "creation of governance capacities…[and] entails the dismantling and reformation of old organizations and institutions–legal, administrative, economic as well as social–the improvement of efficiency and effectiveness of existing institutions, the restoration of destroyed institutions and the enhancement of authorities' professionalism."[196] Psychological and information operations are social and technical approaches to inform and influence mass audiences and targeted actors to shape perceptions and institute behavioral changes[197] such as dissuading violent attitudes or inducing uncertainty or distrust into a group's cohesiveness. Rehabilitation and reintegration are methods of taking responsibility for re-inclusion of known extremists into non-violent society and coaching and mentoring their way back into mainstream life.[198] Lastly, intelligence monitoring is a broad range of activities involving all-source intelligence collection and analysis and paying attention to host nation domestic and international dialog and broadcast and print media for indications of progress of efforts to moderate extremist ideologies and tamp down levels of violence. For my purposes here, I also include intelligence operations as a part of monitoring. Intelligence operations are "tasks undertaken…to obtain information and satisfy validated [intelligence] requirements"[199] and can be quite complex operations in their own right. It must also be noted that many activities within different parts of a host nation society–and different activities within the same sectors of society–will have their own unique levels of access and placement. Thus, every operation within every line of effort that is part of the overall intervention campaign can be used for its intelligence collection value. Everything contributes to the total analysis picture.

C. COMMENCING SONAP ANALYSIS

Analysis of a dark network and how it relates to its environment starts with a set of working hypotheses that prescribe further information necessary to start the opening phases of intervention.[200] Figure 28, from the end of chapter 4, can assist in the development of initial information requirements, given some level of information about the target network. If existing information does not suffice for good analysis, given Krebs' assumptions, then further refined information requirements, or IRs, must be developed and coordinated with collection assets. It is with this framework that we begin analysis and intervention against Noordin Mohammed Top's dark network in Indonesia.

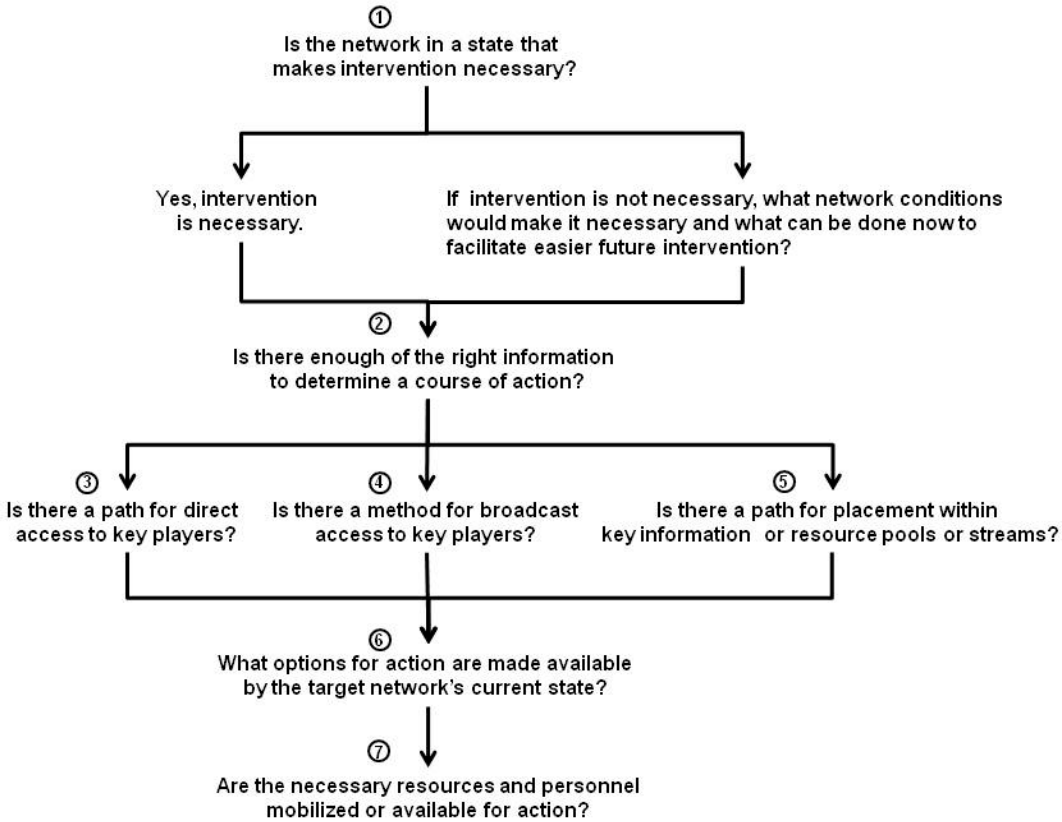

Figure 28. Introduced in Chapter IV, the threat network intervention decision tree can assist in the initial formulation of hypotheses to begin analysis.

D. CASE STUDY: NOORDIN'S TERROR NETWORK

Indonesian authorities killed Noordin Mohammed Top in September, 2009. Prior to then, he formed an effective terror network from a collection of members of different Islamic extremist and traditional Indonesian insurgent organizations. The most notable of was Jema'ah Islamiyah, or JI, which has ties to the Arab core of the al-Qaeda network in Afghanistan dating back to the days of jihadist resistance to the Soviet occupation. The United Nations added JI to its list of organizations and individuals connected to Al-Qaida in 2002.[201] The overall hybrid network that Noordin formed included members of numerous other Islamist organizations, but also followed familial ties, relations between business associates, and friendships between school mates dating back more than a decade.[202] The resulting analysis of these relationships and interactions culminated in the datasets that form the root for this chapter's case study. The remainder of this chapter relies heavily upon the 2006 International Crisis Group document *Asia Report No 114 Terrorism In Indonesia: Noordin's Networks*. The derived datasets are also sourced entirely from this same document, referred to as ICG or ICG sources throughout the remainder of the chapter. Some limitations of this dataset prevent full analysis of the network as described in chapters 3, 4 and 5. Here, this fact is considered part of the inherent difficulty of intelligence collection and imperfect information about dark networks.

Figure 29 depicts the structure of Noordin's Network as derived from the ICG documentation as of May 5, 2006. All 79 known members of the fullest membership of the network are depicted. The column of 9 isolates adjacent to the photo of Noordin depicts known network members, but whose direct links to the main component of the network are unknown. The members and relationships depicted are a 2006 snapshot and, for our purposes, considered the current state of the network. The environmental situation surrounding the network is absent from the graph. However, according to the 2006 ICG sources, the network at that time appeared to be "running short of money and experienced cadres," there was a loss of resources for ideological consultation, Noordin himself was on the run, and there were few trained members who could continue their work without significant assistance. Much of the core of Noordin's network remains at-large, though overall network attrition is very high. The further determination is that the pre-existing networks Noordin drew upon—JI membership and the school networks—will continue to serve as sources of potential recruits. The ICG also notes Noordin's distinct preference for reaching out to small groups who have decided to go it alone. This is the attitude Noordin himself appears to have taken and may play significantly into a future strategy and intervention approach.

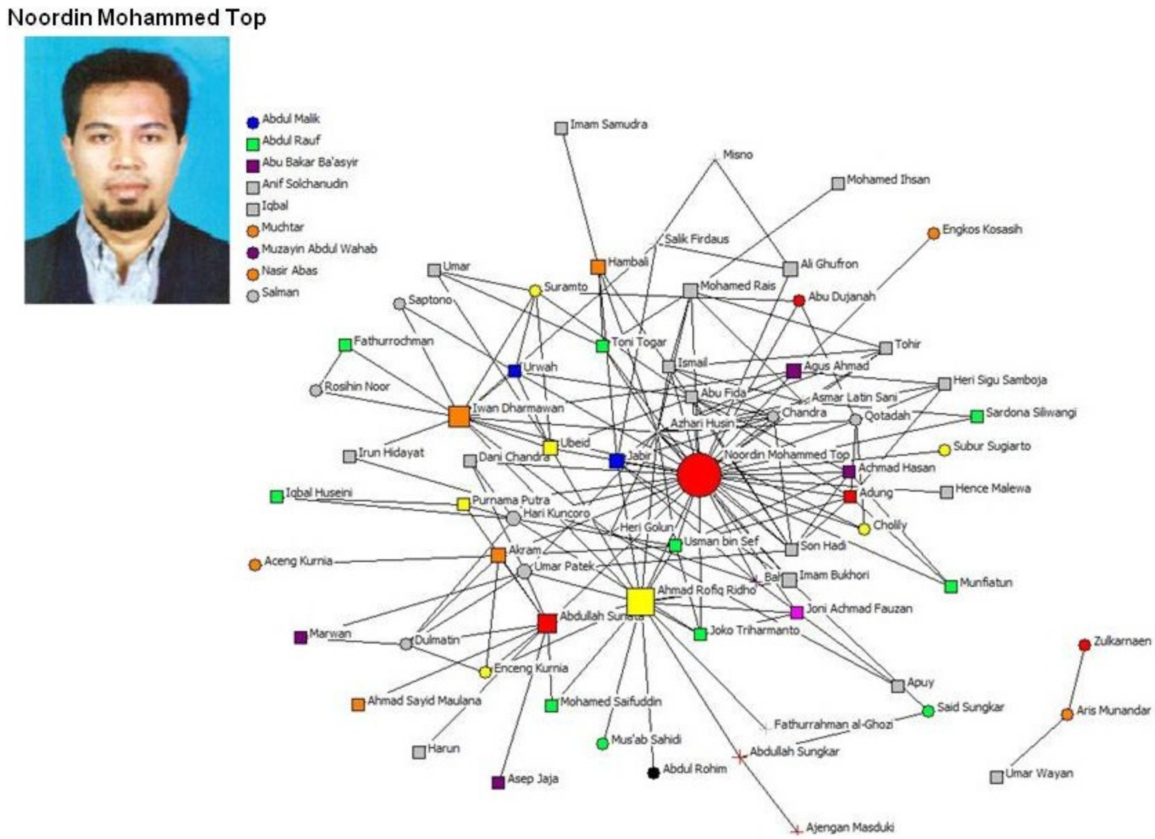

Figure 29. Noordin Mohammed Top, leader of the network depicted and responsible for terrorist attacks in Indonesia, 2003–05. Noordin's place in the network is depicted by the large red circle in the middle.[203]

The four infamous attacks perpetrated by Noordin's followers between 2003 and 2005 brought pursuit and punishment for network members and the resulting attrition from military and law enforcement operations against them have taken their toll (see the surviving membership in Figure 30). By 2006, nearly 70% of the total documented membership had been either killed or detained, with several receiving substantial prison sentences. The remaining 24 members are highly fragmented into several components, most of which are isolates as far as the data indicates, perhaps indeed isolated from one another. There is one main component containing several of Noordin's key associates with Noordin himself remaining the most central figure. For our purposes here, this is the set of initial conditions which set the stage for analysis of changes and development of an intervention strategy. Within these initial conditions, there are some aspects of this data that are significant to an analyst looking to answer the first few questions on the network intervention decision tree.

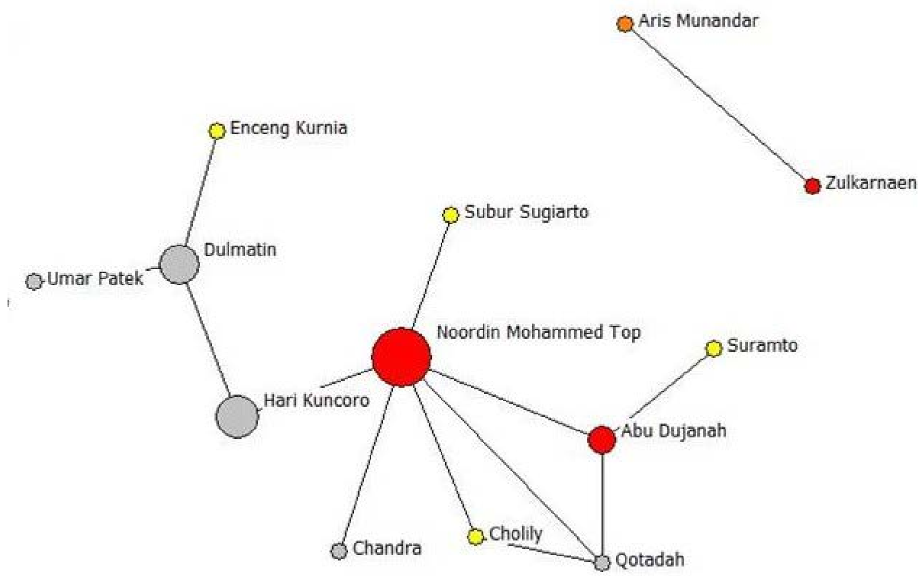

Figure 30. The main component of the current surviving 24-member network, dramatically reduced by attrition due to Indonesian kinetic targeting. This remaining core has proven elusive and, without intervention, resurgence is likely as Noordin reaches out to new recruiting pools.

1. Network State

Question 1. Is the network in a state that makes intervention necessary?

Presuming the Indonesian and regional authorities desire to bring the leaders of this terror organization to justice and to prevent further attacks, yes intervention is necessary. Remembering that Noordin's network was not a casual collection of jihadist groups and Islamic insurgencies, but that Noordin himself purposefully stitched the group together through trusted prior contacts—strong and weak ties—predominantly from Islamic schools, prior jihad experiences, and familial and friendship ties. Those strong ties are composed of trust and energy in motion; and in the weak ties lay network-expanding potential. That same potential exists today as it did before the first attacks in 2002, but with the added attraction of recent success in waging violent jihad against icons of perceived Western influence and decadence. Action-seeking individuals will gravitate to a group that exemplifies their ethos; thus the network will likely grow again. In retrospect, not only was it possible that Noordin's network would re-constitute and resume acts of violence, it did.[204]

2. Information Availability

Question 2. Is there enough of the right information to determine a course of action?

We have information concerning the past and current network structure, we know some of the manner in which the network was partly dismantled, and from that we have a notion of what is missing from the earlier, unimpaired network. Using the dark network mechanisms and functions framework provided in Chapter V, we can identify some of the now defunct systems within his network and some of the systems in which Noordin's network was and is embedded. There is limited information about the macro- and meso-networks between groups and external entities directly related to Noordin's network, and a fair amount of information about the tactical level of network membership, relationships and activities. Analysis of those levels of interaction reveals the social systems which jihadists such as Noordin create and maintain for their cause.

3. An analysis of Noordin's network neighborhood: the inter-organizational level

Noordin assembled his network from a wide variety of backgrounds, particularly exploiting several jihadist organizations and schools. Figures SSS and TTT illustrate the interlocking associations of several entities that served at the strategic level to maintain the health of the jihadist economy of South and SE Asia. Noordin and many of his contacts also drew upon these organizations for recruitment of new members via trusted pre-existing relationships. These groups ranged from formal, western universities to jihadist camps-for-kids-turned-madrasas to well-established ethno-religious armed rebel groups and terrorist organizations with histories and narratives all their own. Further investigation of these institutions reveals opportunities and vulnerabilities for both Noordin and the Indonesian government.

These institutions are similar in that the new recruits and resources came via vetted and trusted sources, though not always native to Noordin's network. Many had their bona fides confirmed via family or friendship ties that went back years—including roots as varied as childhood pals or prior combat experience in places like Afghanistan. The jihadist organizations have focused on creation of an Islamic state in Indonesia and the whole of Oceania (Singapore, Indonesia, Malaysia, Brunei, southern Thailand and southern Philippines).[205] The schools are focused on education and indoctrination for the very long term outcome of multi-generational mobilization. In Noordin's experience, drawing heavily from complimentary institutions has paid off.

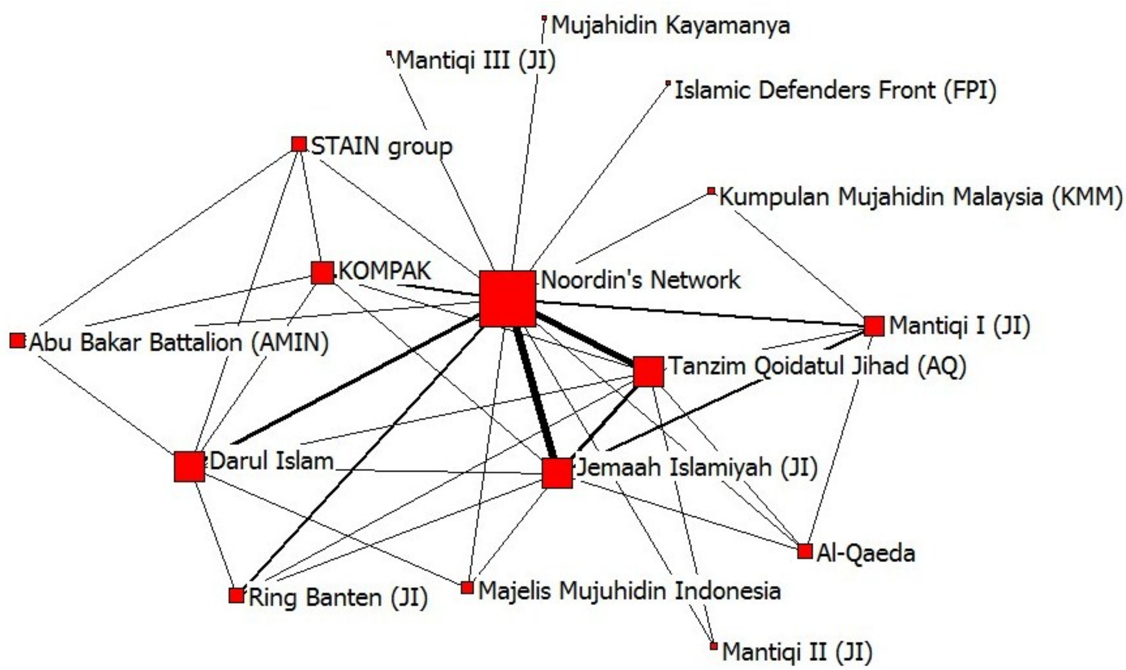

Figure 31. Noordin's network neighborhood at the group level. Node size indicates degree centrality: the larger the symbol the higher the relative degree centrality. Link thickness indicates the relative amount of mobility of membership between organizations. Note the multiple entities that share JI lineage or subordination.

The adults that came from the meso-level inter-organizational networks came with a wide range of experiences that fed into the health of Noordin's organization. Figure 31 shows that the primary organizations that fed Noordin's network were JI, al-Qaida, and two older, traditional Islamist groups: KOMPAK and Darul Islam. Some of the other groups depicted—Mantiqi I, II, and III and Ring Banten—are actually administrative or geographical divisions of JI, and JI itself is an historical off-shoot of Darul Islam.[206] That means that there are long-standing ties between organizations beyond just membership mobility.

Many members of Noordin's network traced their ideological lineage via shared mechanisms such as combat or school attendance and some came to value the new attachments over their previous relationships. In so doing, they demonstrated altered loyalties–re-directed trust–to their new organization over their previous attachments. A post-Marriott bombing episode with Toni Togar exemplifies this: getting cold feet as he stored all the left over explosives at his house, Togar chose to call Noordin to tell him that he was going to "throw them out" rather than his immediate JI supervisor. While the ICG documentation does not explain why this happened, the implication is that Noordin's action-oriented ethos drew higher levels of trust than the prior long-standing relationships.[207] Many of those interlocking relationships are depicted in Figure 32.

So, we have not only determined that some sort of JI or other Islamist credentials are a must for anyone seeking to enter Noordin's network or to associate with its members, but also that infiltration of one group may enable infiltration of others, including Noordin's. We also know that individual choices by dually-employed members in mechanisms shared between more than one network can disrupt one organization's control over the mechanisms and the members of it. This is the essence of principal-agency problems and may indicate an opportunity for intervention.

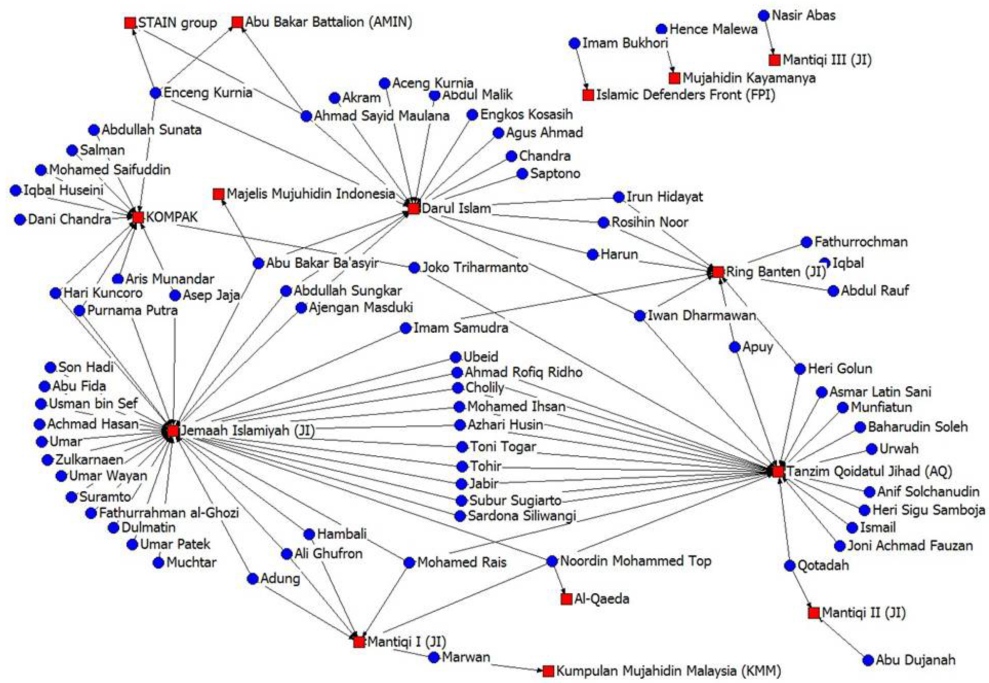

Figure 32. A graph of all of the interlocking associations across Noordin's jihadist economy in Indonesia. Jemaah Islamiyah, al-Qaeda, Darul Islam, KOMPAK and the JI subsidiary Ring Banten are the largest contributors of members to Noordin's operations and supporting mechanisms. Organizations are represented by red boxes, members are blue circles.

Not all schools are equal when it comes to contributions specific to Noordin's campaign. Figure 33 illustrates that Pondok Ngruki (al-Mukmin) and Luqmanul Hakeim are the primary feeder schools for membership in Noordin's endeavor. Two other schools of note are the Universitas an-Nur and University of Technology of Malaysia. Noordin himself was a product of the University of Technology and Luqmanul Hamkeim.

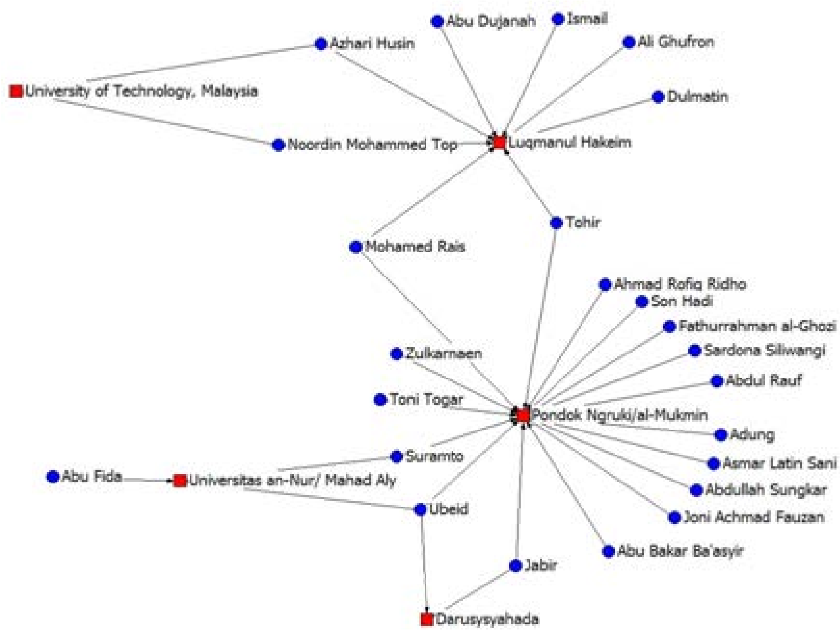

Figure 33. A graph of the Islamic school associations within Noordin's network. Pondok Ngruki and Luqmanul Hakeim were particularly instrumental in providing indoctrinated graduates into the jihadist economy in SE Asia and Oceania. Schools are represented by red boxes, members are blue circles.

Again we see that membership mobility is a useful perspective in that these institutions can feed into one another. Students in school graduate and join the adult organizations, and those adult organizations send skilled members to be teachers and mentors at the schools. This sort of mobility may provide an in-road into the Indonesian insurgent-terror economy, as long as there is enough of a perception of the right kind of biographical history to support placement in what may be otherwise privileged tutelage. That sort of capability demands special agent selection criteria and development. And, despite the fact that a child would never be suspected of being an intelligence agent in a school appropriate for his age, employment of children in any capacity is strictly forbidden.

Degree	Closeness	Betweenness	Eigenvector
Pondok Ngruki 42.86	**Pondok Ngruki** 63.16	**Pondok Ngruki** 43.96	**Universitas an-Nur** 69.11
Universitas an-Nur 42.86	**Universitas an-Nur** 57.14	**Universitas an-Nur** 30.77	**Pondok Ngruki** 68.98
Luqmanul Hakeim 28.57	**Luqmanul Hakeim** 50	**Luqmanul Hakeim** 29.67	**al-Husein** 50.22
Adelaide University 21.43	**al-Husein** 48	**al-Muttaqien** 12.09	**Indramayu** 50.22
al-Husein 21.43	**Indramayu** 48		**Darusysyahada** 36.83
al-Muttaqien 21.43	**Darusysyahada** 46.15		**Luqmanul Hakeim** 33.89
Indramayu 21.43			
Reading University 21.43			
Univ. of Technology, Malaysia 21.43			

Table 2. The centrality scores of the Islamic schools. Centrality scores for the Pondok Ngruki school, the Universitas an-Nur and Luqmanul Hakeim school indicate a starting point for where to focus intelligence collection (monitoring), institution building, psychological operations and information operations (from Roberts and Everton, 2011).

Roberts' and Everton's[208] analysis of the Indonesian-based meso-networks between members of Noordin's network and the Islamic schools they attended (Table 2) provides focus and insight into the recruitment and ideology mechanisms. Still, a full CARVER analysis of the schools that contribute to violent jihadist narratives is not possible due to lack of information that relates the various schools to one another. Analysis of the trust networks between network members and the geo-spatial basis of their relationships highlights the centrality of Islamic schools in their recruitment and ideological experiences. In Noordin's case, the Muslim schools were critical to the future structure of trust and social capital for his network.

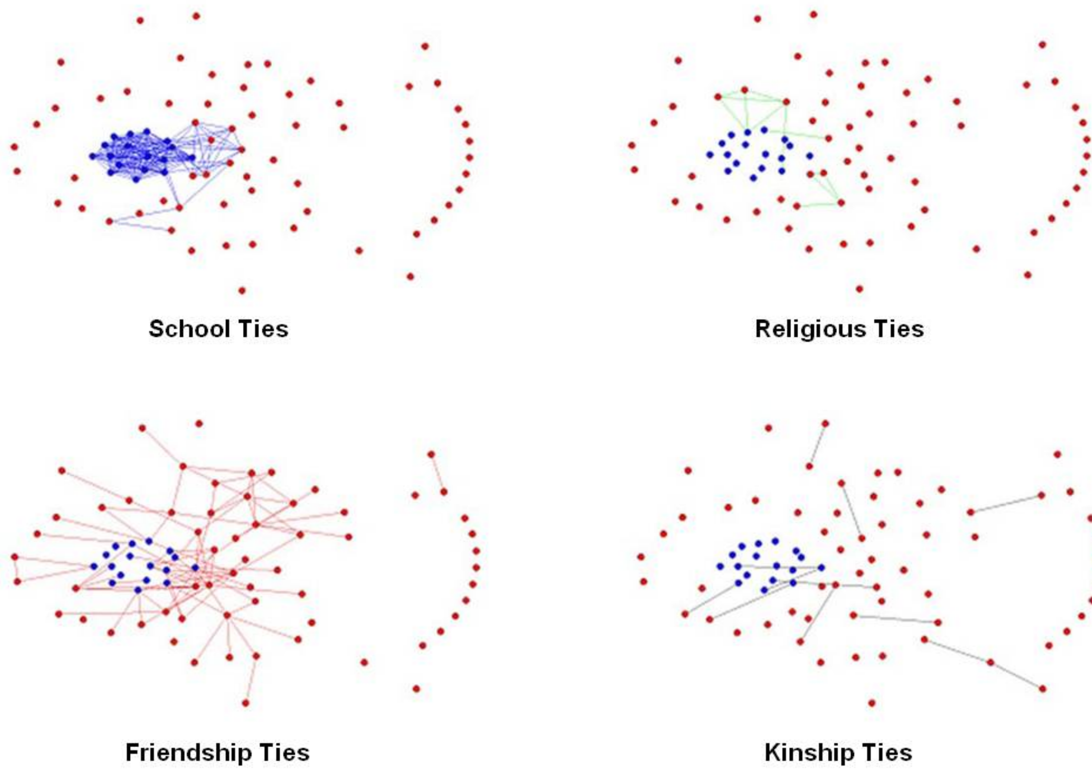

Figure 34. Densities of relationships within different types of historical ties between members of Noordin's network. The school ties have been critical to the internal cohesion of Noordin's network (from Roberts and Everton, 2011).

From Figure 34, we see that school ties have played a significant role in the formation, ideology and unity for Noordin's network. The tight web of connections between members based on school ties is not reflected anywhere else. Thus, the data about school attendance provides a basis for describing the meso-networks between individuals and between groups. Further analysis of the meso-network of Islamic schools, also completed by Roberts and Everton, reveals that three schools played significantly greater roles in the growth of the network. As shown in figure NNN, the Pondok Ngruki, Universitas an-Nur and Luqmanul Hakeim schools are at or near the top of most measures of centrality. We now have two focus areas for consideration for intervention. Lastly, there are a large number of network members, both in and out of prison, who likely retain contacts outside of Indonesia. Further analysis of those ties reveals a larger pool of points of entry to Noordin's network, but none as clear as the school and organizational ties.

In summary, understanding Noordin's network neighborhood gives insight into the mechanisms of recruiting, resourcing, sanctuary and intelligence collection. A holistic view of the structure and relational dynamics at work in the network's external environment—its network neighborhood—is just as important as understanding those aspects of its internal operating structure and environment. Now that we understand some of the context of Noordin's embeddedness in his environment, we look inside his operating world.

4. Assessing the Damage: A Functional-Loss Analysis of Noordin's Network

As of 2006, all of seven dark network functions are severely damaged. Some functions which we know were still at a partial level of functionality are leadership, sanctuary, and recruiting. We know that these were in some semblance of working order because Noordin and what remained of his core membership were successfully hiding and trying to reconstitute the organization. However, there were indications that the other functions (ideology, operations, intelligence, and resourcing) were diminished to the point of non-functionality or may not have been functioning at all in order to preserve those capabilities for later use. In fact, they have all been greatly diminished, presuming that the available data is representative of the real situation.

An analysis of what remains of the various functions will highlight some useful aspects of the network's current state and associated opportunities for counterterrorism efforts. There are two parts to this functional-loss damage assessment. The quantitative assessment indicates the numerical comparisons of what exists now to what existed in the fully-functioning network. A percentage of the former capability is used as an indicator of effectiveness. The other side of the coin is the qualitative assessment, which requires a much more in-depth look at more variables per member: the individual roles of members within the mechanisms, their total commitments to roles in multiple mechanisms or roles within the same mechanism, previous experiences and training, length of time in the role and position in the mechanism, and robustness of range of options for resources in that role. Other aspects of the member's experience may be unique to that person's experience or background.

One structural hole theoretical approach to this depth of analysis is that the heavier workloads will require more experience and more options for resources (fewer structural holes between the member and resources necessary). If a member has multiple roles in multiple mechanisms (too few structural holes) and member attrition in one or more mechanisms occurs, then task overload may lead to exhaustion and the mechanism may shut down temporarily until tasks can be re-distributed, or be lost altogether. Obviously, Noordin and his subordinates want to avoid that at all costs, and this may be exploitable by counter-terror agencies.

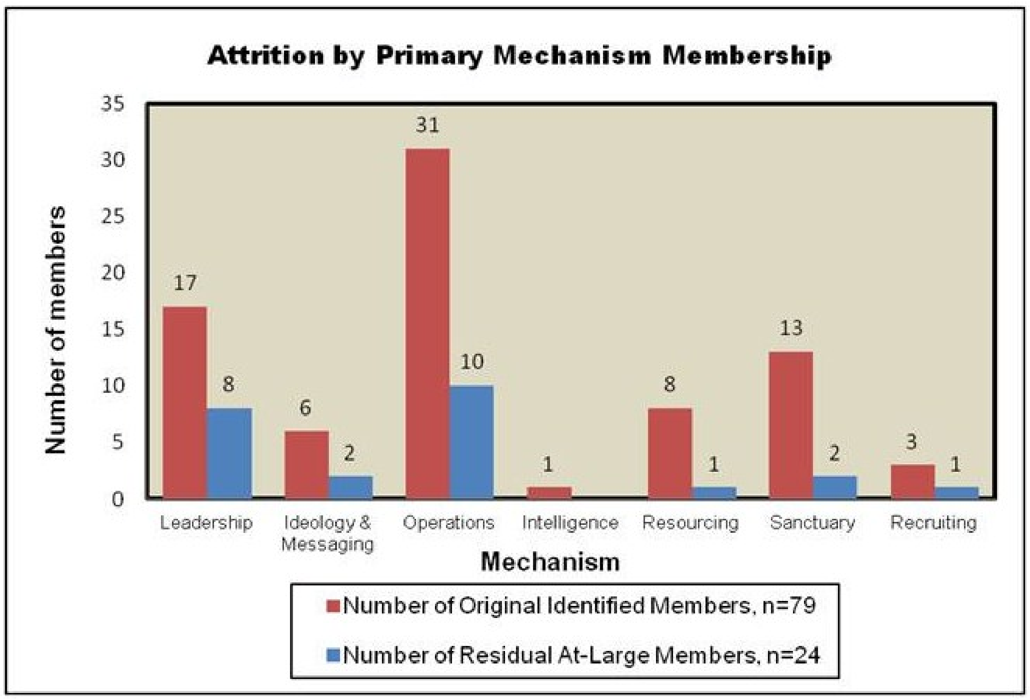

Figure 35. Losses to the network overall were severe, but attrition of assets available to certain mechanisms were nearly total. Leadership remains the most intact mechanism, but most others were made completely ineffective in supporting terror operations of the scale seen in 2005.

In the quantitative analysis, the most basic comparison is what exists now as compared to what existed in a fully-functioning network. This analysis is broken down by mechanism/function for better fidelity of systemic degradation. Figure 35 shows the net losses of each mechanism across Noordin's network. Despite 70% recorded losses overall, Noordin's leadership and operational mechanisms fared the best, with about 50% and 30% survival rates, respectively. Most other mechanisms are reduced to ineffectiveness due to attrition and loss of cohesion amongst the remaining at-large members. Obviously, the unknowable facts concerning who is in actual contact with whom and what they are able to accomplish together are many, but it is safe to say that severe damage to Noordin's network was accomplished by 2006. Also, the fact that Noordin's network has not been able to conduct any terrorist attacks in this current state gives strong indications that there are multi-functional dependencies at play. Even though there are more operational mechanism members surviving and at-large than any other two mechanism combined, the other mechanisms collectively cannot provide sufficient support to conduct operations. The task at hand now is to prevent any recurrence and continue to pursue the survivors until dead or brought to justice, or both. First, to better understand the capabilities, capacity and vulnerabilities that exist, we analyze what remains of the mechanisms.

a. Leadership and decision making

Leadership and decision making were still largely intact because Noordin and a few other mechanism members were still at large. Even though he lost many of his immediate subordinate leaders, such as Abdullah Sunata and Adung, Noordin is the creator and primary driver of the network and was seeking to expand his network to be at least as capable as it was before attrition. Figure 36 depicts the current core leadership situation as Noordin and only two other leaders or strategists, Abu Dujanah and Zulkarnaen, remain at large. However, exactly how Zulkarnaen collaborated with Noordin is hard to determine from the documentation.

b. Ideology and messaging

Bona fide experts in violent jihadist narratives from Jema'ah Islamiyah and other radical Islamist ideological sources are in short supply for Noordin. Prior to his arrest and receiving a death sentence, Ali Ghufron, aka Mukhlas, provided nearly all the jihadist literature and opinions for the inner group.[209] He is now in jail, though not completely isolated from the outside world as Indonesian prisons are not known for their security.[210] Noordin was searching for a new spiritual leader who can assist the members along their jihadist path. JI relied upon their own spiritual branding of jihad to differentiate them from the other Islamist groups in the region, and Noordin's group was an off-shoot of JI.[211] He may return to his JI contacts for another spiritual guide.

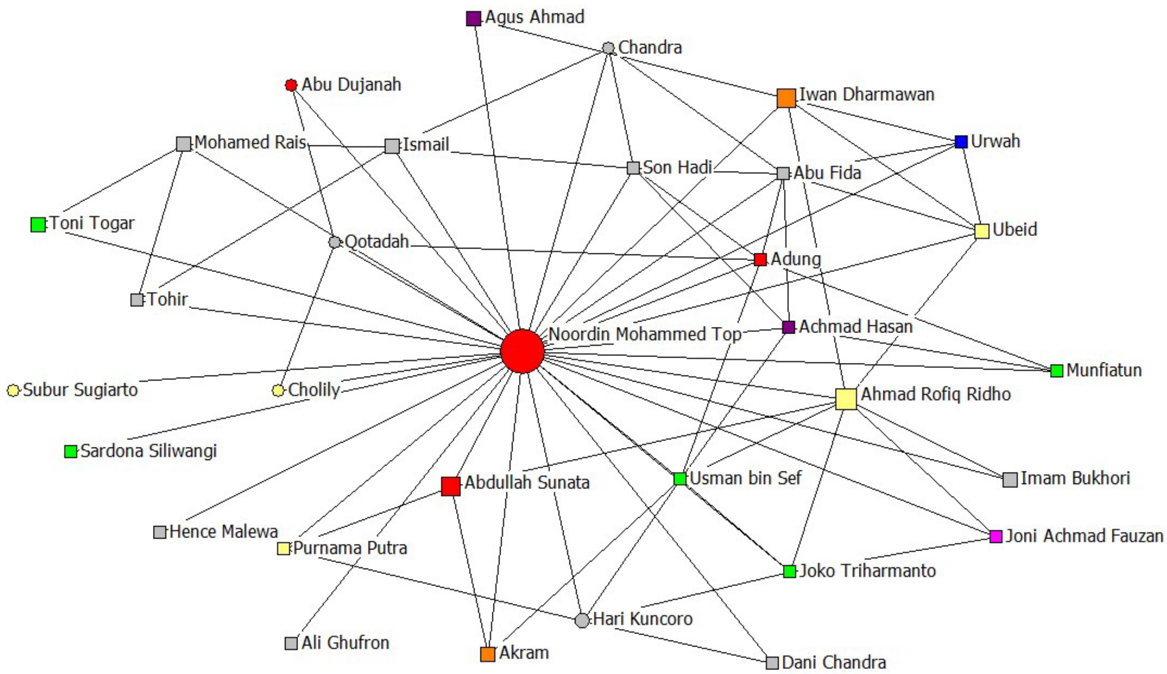

Figure 36. Noordin's 2006 ego net—all of his direct ties—reveals many lost members who were key to his campaign. Noordin remained at large with Abu Dujanah, the only other leader or strategist. The square nodes represent the incarcerated members; members who were free in 2006 are represented by circles. Red indicates a leadership or strategist role.

c. Operations

The operations mechanism fared moderately well through the period of attrition, retaining about one-third of its strength (31 members decreased to 10). Included in the operations mechanism are the members who actually conduct attacks, the instructors who trained fighters and suicide bombers, the bomb-makers, and limited membership who performed multiple other operational support functions as couriers or transporters. As these men were the action arm of the network, they possessed no independent resourcing or sanctuary sub-systems of their own. As noted, there was some limited role-sharing with other mechanisms, but they are completely dependent upon those two mechanisms for the base of operational material supplies and safe havens in which to hide from the authorities, prepare for missions and recover from actions.

d. Intelligence

Of all the mechanisms, we have the least amount of information of members primarily employed in intelligence collection. There are a few of the actual attackers (operations mechanism) who also conducted their own reconnaissance and surveillance of targets and some recruiters also did some reconnaissance work, but information is sparse concerning those members whose primary purpose was to collect intelligence and provide it to Noordin or to the network as a whole. The one member assessed to be most uniquely concerned with target reconnaissance—Joni Achmed Fauzan—was sentenced to prison for six years.[212] He had two assistants, but they are accounted for in other mechanisms (the aforementioned recruiters). Two of the chief ways to defeat reconnaissance and surveillance is to harden the target, conduct some kind of vetting of employees, and active surveillance countermeasures, thereby creating a paucity of information sources available to Noordin makes this task all the easier.

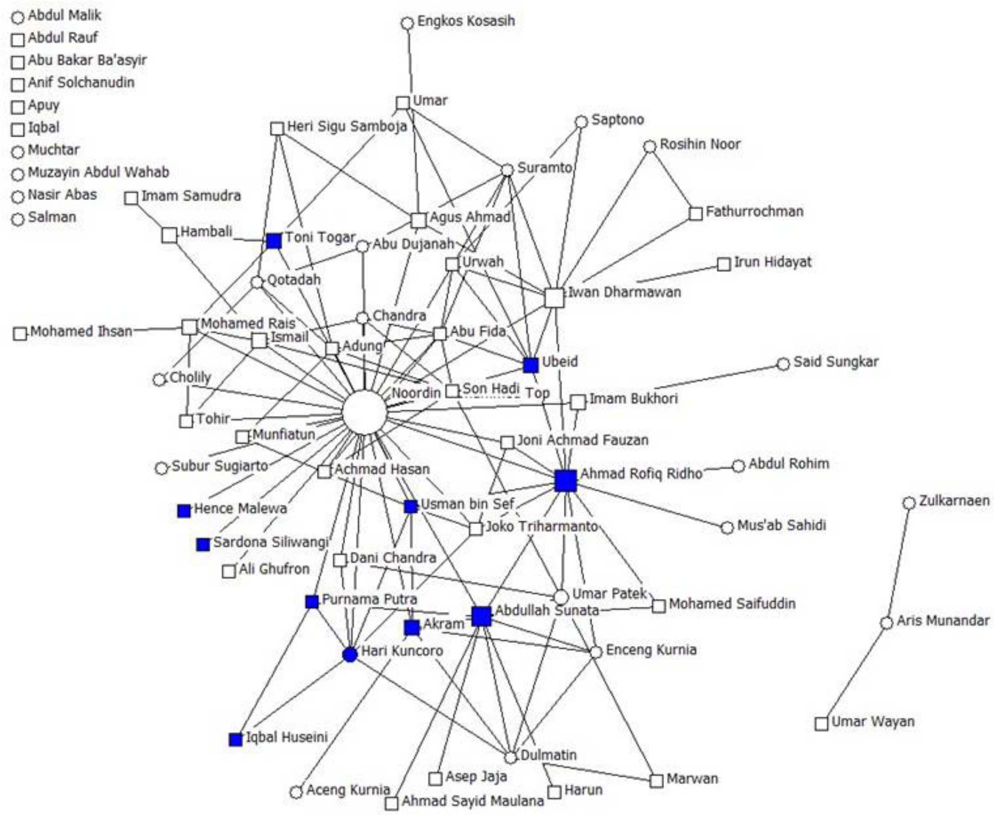

Figure 37. Noordin's original network graph highlighting members associated with the weapons procurement function. The box-shaped nodes are those members who are incarcerated; the only remaining active member is Hari Kuncoro, represented by the circle-shaped node near the bottom of the graph.

e. Resourcing

Another severely diminished function is resourcing. Specifically, the weapons procurement function (Figure 37) is completely defunct, as are most of the financing cells (Figure 38). Often, the provider of materials was also the transporter and the one who maintained the explosives and weapons caches on their own property. This may have played a significant role in finding, arresting and prosecuting these multi-role supporters as—there may have been too few structural holes (too little compartmentation) of roles and functions. In manner of speaking, as the Indonesian authorities began to effectively counter the network and detain members based upon interrogations of previously detained members, any network member who took on too many different roles in different mechanisms became a liability instead of a multi-tasking asset. Consequently, when members like Purnama Putra, who had roles in three separate subsystems within the resourcing mechanism and direct relations with several other members who were all within one or two degrees of Noordin, his capture elevated personal and operational risk substantially.

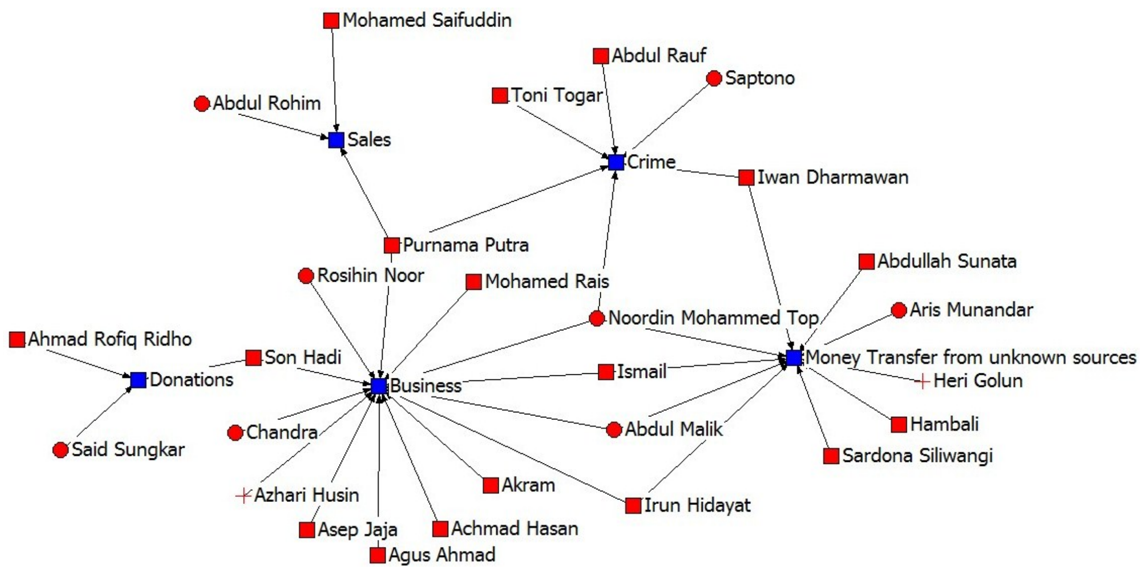

Figure 38. Members of the illicit financing sub-systems within the resourcing mechanism, by subsystem. This graph depicts all members who were full-time and part-time involved in financing, according to the ICG documentation. The box-shaped nodes are those members who are incarcerated; the circles represent at-large members. The two "+" signs represent deceased members.

f. Sanctuary

The sanctuary mechanism is badly damaged. Of the 13 original members, only two remain at large. Because of the risk of a single catastrophic compromise of multiple members residing at one location, a robust mechanism of safe houses, caches, and other safe sites is a necessity. And, unless there is a large swath of terrain or urban area that remains ungoverned or controlled by the network or a patron of the network, then the safety of network members cannot be guaranteed without a deep bench of vetted and tested safe houses. Sanctuary systems are not designed with a 1:1 member-to-safe site ratio in mind, but rather the network of safe sites is supposed to be both deep and wide, so key network members are able to maintain some level of ambiguity as to their location on any given night. So, as the covert network membership and material supply increases, so must the capacity of the sanctuary function. That means numbers of safe houses and safe house keepers and others who assist wittingly and unwittingly in the maintenance and support of a safe house must also increase. A safe house is not just an apartment in town; it is another layer of systems that must be carefully constructed and controlled within an agreeable network and physical neighborhood or with an enormous amount of energy spent maintaining a secure and consistent cover.[213] This is not easily accomplished even by skilled and experienced managers—and failure to create a sound sub-network of safe site may have contributed to the success of the Indonesian authorities up to 2006 and afterward. Figure 39 illustrates the 2006 situation regarding the sanctuary function. All but two members of the network associated with safe houses are incarcerated.

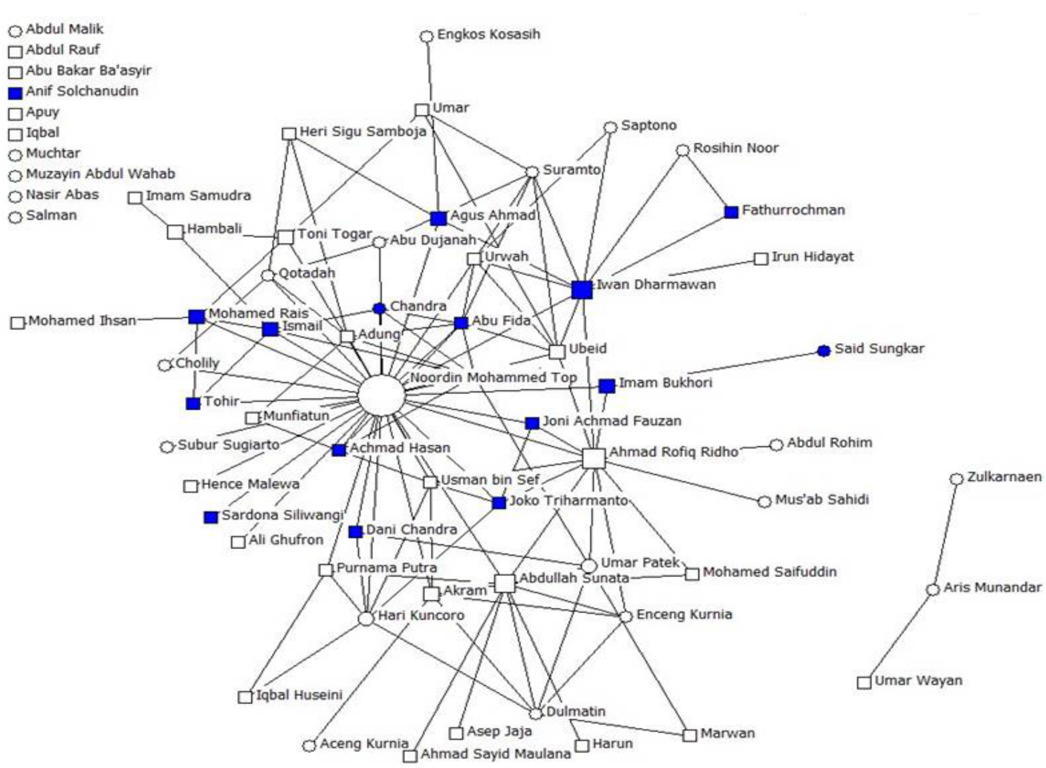

Figure 39. Noordin's original network graph displaying the damage to the sanctuary function. All blue-colored members had a role in the sanctuary mechanism. The box-shaped nodes are those members who are incarcerated; the only two remaining at-large are Chandra and Said Sungkar the circles.

In the final analysis, the tremendous losses incurred within the sanctuary and resourcing mechanism created huge structural holes and many new isolates. Over-embeddedness—being a member of too many mechanisms simultaneously—may have contributed to the demise of some members. But Noordin is the chief exception to that idea: he was embedded in several mechanisms while chiefly playing the roles of strategist, decision maker and recruiter. He may well have learned from his mistakes and may consider building in better compartmentation as he re-builds his network; that is to say in network terms that he ought to build in more structural holes and other safeguards against compromise of brokers and gate keepers between cells and mechanisms.

g. Recruitment.

Significant recruitment occurred primarily by Noordin's personal actions or personal references of his bringing prospective new members into the fold. There were a few members who spent part of their time, at least from what the ICG documentation describes, as limited recruiters. However, what may be different now, is that trusted members who were directly recruited by Noordin or his top deputies are now in prison. Their qualifications and trust may or may not be diminished, but they may play an important part as references for candidates who are about to be released from incarceration. These men will play an important part of our infiltration scheme.

5. A Systems and CARVER Analysis of Noordin's Network

Remembering that the CARVER method of analysis is an acknowledgement that systems are built upon systems, it follows that a systems understanding of the task at hand is required. In our current range of documentation, there is limited information about the larger jihadist economies in SE Asia and Oceania. A complete CARVER analysis of Noordin's networks is not possible because the relational data about the jihadist meso- and macro-networks outside of Indonesia and between surrounding layers of traditional Muslim organizations are unavailable. However, we do have an understanding of the systems within Noordin's networks, their purpose, and where some of them originated. Figure 40 depicts a simplified interpretation of the operational-level system at work in Noordin's terror campaign.

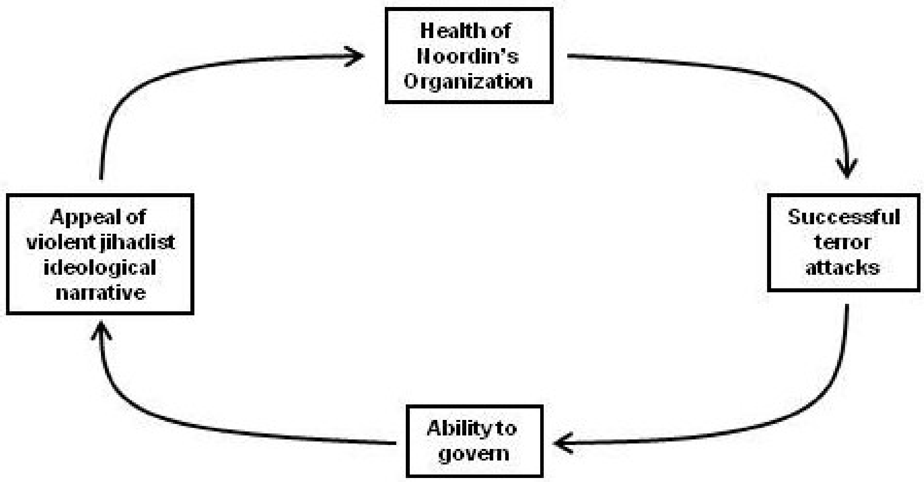

Figure 40. The primary system at work in Noordin's terror campaign may be referred to as a terror success cycle. Success at each point has a positive influence on the next. A CT campaign must break that reinforcing cycle.

In this simple system, successful terrorist attacks detract from the population's perception of the Indonesian authorities' legitimacy and ability to govern. That inability to govern becomes realized as people withdraw participation and seek alternative authorities and narratives that align more closely with their needs. Islamist narratives such as JI's call to jihad and vision of a wider Islamic state and future caliphate resonate with a portion of the Indonesian population. As that sentiment grows, jihadist organizations such as Noordin's benefit from the increased mobilization of recruits and resources, particularly if the original attacks can be attributed to certain organizations. Subsequent iterations of this cycle reinforce the social dynamics instigated by the previous iterations. Advantageously for groups like Noordin's, mobilization becomes an absorption capacity problem and groups require channels in which to funnel the recruits, resources and increased social capital. Figure 41 is a more complex systems view of Noordin's terror campaign comprised mostly of the internal systems and the major external system they seek to influence.

In the next lower level of analysis—an internal or tactical systems view—we see the seven dark network functions come into play. When popular appeal of jihadist narratives and proposed solutions begin to overtake government influence (due to diminished support for Indonesian governmental control) people may begin to take a greater interest in the action behind the narrative. With this interest, not only does the number of prospective recruits increase, but so do volume and types of resources as well as opportunities for expansion of operations. Successful exploitation of the new popular interest will allow the network leadership the space to determine how best to continue to prosecute their struggle against the authorities: to change nothing, to expand direct control (centralize), or to release some level of control (decentralize) to allow subordinate networks to operate more freely.

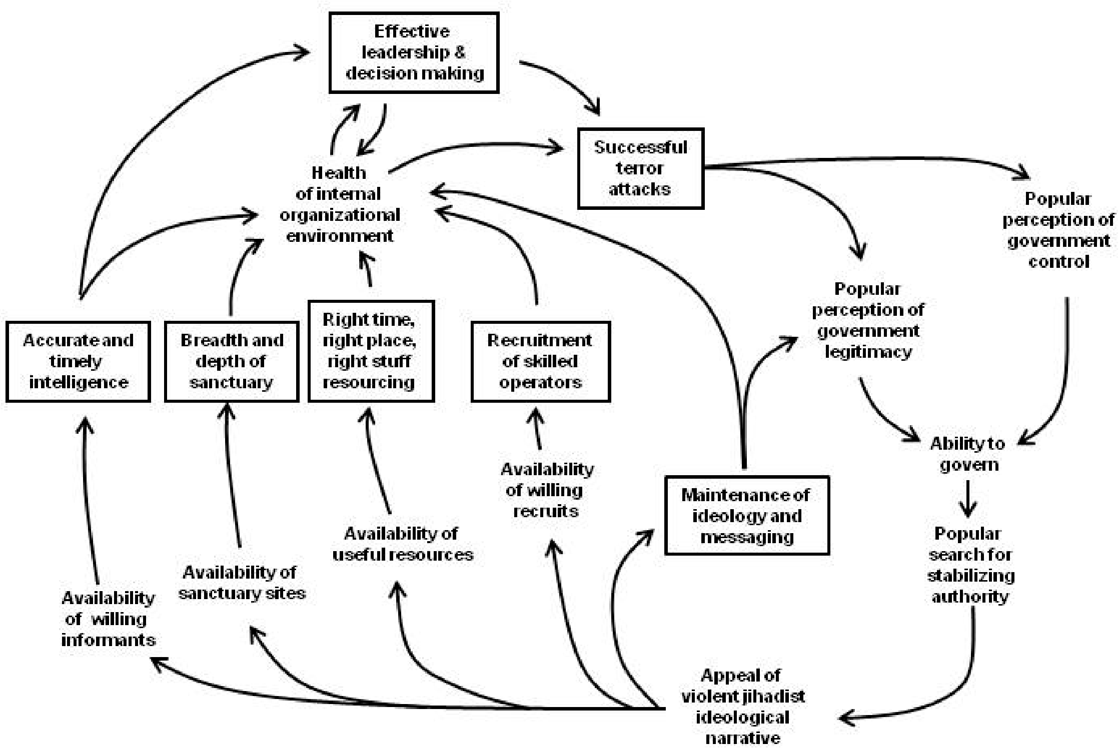

Figure 41. A systems view of Noordin's terror campaign focusing on his network's functions (in boxes).

Figure 41 illustrates a systems view of these dynamics, with all seven dark network functions able to expand. The seven dark network functions all contribute to the internal health of the organization, which culminates in a reinforcing cycle of successful terror operations, diminished state's ability to govern, ideological appeal, and improved health of the organization. So, the internal health of the organization is inversely related to the relative power of the authority. An obvious conclusion is that counterterrorism or counterinsurgent campaigns should culminate not only in preventing dark network attacks, but should degrade the overall health of the network by disrupting the success cycle.

From the data we have, it is possible to map out the relational data both for membership and functions within the context of Noordin's overall terror campaign. CARVER analysis supported by analysis of gaps within the surviving network reveals come critical vulnerabilities. Namely, those are the functions most negatively impacted in terms of ability to support the larger network: ideology, resourcing and sanctuary. But these functions are not equally deficient in the current state of the network. That uneven distribution of lost capability also means there are functions that require much more rapid growth than others. Rapid re-growth can be exploited.

CARVER Application

Mechanism	C Criticality	A Accessibility	R Recuperability	V Vulnerability	E Effect	R Recognizability	Total
Leadership & Decision Making	5	1	5	1	5	5	22
Ideology & Messaging	5	4	2	2	4	3	20
Operations	5	1	2	2	4	4	18
Intelligence	4	1	3	1	5	1	15
Resourcing	4	4	5	5	4	1	23
Sanctuary	4	4	3	5	5	1	22
Recruiting	4	4	4	5	2	1	20

1=lowest, 5=highest

Figure 42. Tactical CARVER analysis of Noordin's network functions. Resourcing and Sanctuary are chosen as the best for tactical targeting. Leadership is also ranked very high, but has the lowest score for accessibility, which stems from the current inability to directly attack Noordin or other leadership figures.

A CARVER matrix (Figure 42) developed from the mechanism attrition assessments depicts values assigned for identifying which systems to target. While all systems may be attacked at some level, Resourcing and Sanctuary are chosen because they have suffered the most damage in terms of support capacity to the overall network. If Noordin and his co-conspirators are to remain free, and restore freedom of movement in order to re-gain access to recruits, resources and targeting opportunities, then they will need to have rapid re-generation of these mechanisms.

6. Key Players

Question 3. Is there a path for access to key players?

No, there is no known direct path from incarcerated members to the members still at-large. Presuming the Indonesian authorities are competently distilling the intelligence they collect and effectively pursuing leads, there is currently no direct path to key members of Noordin's network that presents itself from the ICG documentation. The majority of the peripheral members have been culled from the core and Noordin's remaining contacts appear to be skilled or lucky enough to evade capture. Further investigation of members' backgrounds or more effective interrogation of the imprisoned members may lead to more useful information. However, there are some members who can be theoretically templated as having enough historical social connections that they may be useful. Those members may be elevated in priority for rehabilitation and reintegration programs, and possible recruitment into a program to employ them against their former comrades. In this way, we can construct the necessary network pathways to give us the access and placement we need to prevent attacks and bring an end Noordin's terror campaign.

7. Broadcast Access

Question 4. Is there a method for broadcast access to key players?

Yes. Even if the surviving and at-large members went underground, they are likely not totally isolated from the effect of mass media. These members and their supporters do not live in a bubble. Merely surviving, they must still receive aid from supporters such as sanctuary, food, water, information, and communication via cut-outs and intermediaries between one another. If they seek to re-constitute an effective action network, then even more communication and flow of resources and personnel must occur. The same roadside signs and establishments that psychologically impact innocent travelers also impact the members and their supporters. Local chatter around watering holes, eating establishments and other businesses is openly shared with all who pass by. Previously untapped resources are already influenced by information passed by television, radio, printed media, the Internet and word of mouth. If Noordin and his top surviving lieutenants are indeed rebuilding their network to some semblance of its former self, then they must reach out, risking identification and compromise or capture. There is certainly room for psychological and information operations to inform and influence local populations in the vicinity of suspected sanctuary regions, such as central Java. Short of utter isolation, information distributed via broadcast means is sure to reach Noordin and his people, and guaranteed to reach his potential future accomplices who live in the region.

In today's increasingly technological world, using any level of electronic technology for communication, navigation, or computing very nearly automatically means a certain vulnerability to electronic exploitation.

8. Access and Placement

Question 5. Is there a path for placement within key information or resource pools or streams?

Yes. This requires an in-depth look into the mechanisms that comprised Noordin's fully-functioning network of 2002–2005 and determine what is necessary and sufficient to reconstitute an effective insurgent or terror organization. To do this, we examine the full network of 2002–05, subtract what has been dismantled or degraded and compare to an idealized model of network structures that supports a healthy and effective organization as described in Chapter 5. By following historical recruitment mechanisms—trusted jihadist organizations and schools—we can place ourselves within the sanctuary and resourcing mechanisms with the full resources available to state intelligence agencies. Coming to the table with greater resources than other jihadist competition (aka other jihadists with access to various weapons, explosives, safe sites, funds, and the like will assist in tipping the balance to the authorities' favor. The local genuine jihadist resource providers will not be able to compete and will get squeezed out. Infiltrating these critical and (as of 2006) depleted mechanisms means filling the void created by attrition of members and making certain scarce resources available via trained intelligence agents and recruited former jihadis.

The sanctuary and resourcing mechanisms are not random sub-networks which happen to be available. These degraded mechanisms are open wounds in very central functions that touch the core of Noordin's network. Key players must live somewhere safe, and operations cannot be planned or executed without confidence of resource availability. The result of successful infiltration like this is two-fold. First, the safe site mechanism provides awareness of the movements, patterns and locations of key players. Proper technological surveillance of these sites also notifies authorities of plans and intentions. Second, owning a portion (or the entirety) of the resource mechanism allows a level of control over the timing and method of future operations.

Discovery of the remaining members' methods of communications on the Internet will also provide excellent access to information based on real-time flows of ideas and directives. The anonymity of chat rooms can work against the terrorist as well as in their favor. Identification and exploitation of Internet domains that are utilized by Noordin's people will go a long way toward understanding precisely who is dependent upon whom and for what, and may give indicators as to what kind of cognitive and task loads different members are bearing. Monitoring their communications will also give independent confirmation of other operations' effectiveness.

9. Options for Action

Question 6. What options for action are made available by the network's current state?

There are two perspectives to this question: what is possible and what is not allowed by laws, treaties and agreements. Included in this equation are the internal and external aspects of the network's situation as allowed or constrained by U.S and

Indonesian national laws and international treaties. In that light, there are several approaches available for intervention against Noordin's network and a few that are disallowed. First, an example of an action that would be disallowed under the circumstances for the time period when the ICG document was written. The importance of geo-spatial intelligence—knowing where the enemy is geographically—is obviously important in this example.

Unilateral kinetic targeting when high-value individuals, or HVIs, are inside Indonesia's sovereign territorial waters or land mass requires direct intervention into that nation's sovereignty and is not currently a policy of the U.S. government. Any military action would need explicit approval from the Indonesian government. There is also the option of conducting a covert action, but that requires a Presidential finding which must be specific to the national security of the U.S.[214]

Kinetic targeting of HVIs in international territories such as the open seas or in ungoverned spaces on land, direct intervention is more likely to be allowed from a legal perspective. This would also require a Presidential finding unless special provisions or policies such as a declared war or invocation of the right of self-defense could be established.[215] Other nations' desires may also factor in decisions to intervene. Specifically, Australia would likely have a strong desire to lead or participate in such an action since many of the dead and injured from the 2003–05 attacks are Australian citizens, and particularly for the 2004 Australian embassy bombing.

Here, however, the dark network in question is mostly land-based. The issue is not that there is no precedent for such activities, but that the threshold for authorization for these actions is much higher than in a declared combat zone, and the U.S. had no such policies in place for pursuing Noordin. This is one example of the legal aspects of terrorism, counterterrorism and international assistance against a lethal enemy, in irregular warfare. That being said, there are numerous options that are feasible and contribute directly to a strategic approach to supporting Indonesia's struggle with domestic violent jihad. Every category of action proscribed by Roberts and Everton is on the table:

U.S.-unilateral kinetic targeting in international waters may be permissible. International laws allow for military actions in international waters when the threat falls within certain parameters, particularly when a country invokes its inherent right of self-defense. Whenever contacts of Noordin's—or Noordin himself—can be tracked while transiting between sovereign territories, we are legally allowed to conduct a kinetic surgical strike to kill or capture them.

Kinetic targeting capacity building is a hybrid of the direct and indirect approaches. We can build up the capabilities of Indonesian and regional actors to support law enforcement investigations, domestic and international intelligence collection and prosecutions that support their own kill or capture operations in their own counterterrorism campaign. Ideally, this would be linked to institution building, wherever necessary.

Indonesia's military, legal, law enforcement, and judicial institutions are lagging behind the cutting edge of effective security and governance in the 21st century. The United States' federal government has the means to assist with nearly all aspects of intelligence processes and sharing, counterterrorism, law enforcement, and judicial practices. Many departments and agencies are the disposal of the lead agency, which here ought to be the Department of State, supported by the Defense Department, Justice, the CIA, Treasury, just to name a few.

Psychological Operations, or as is now known as Military Information Support Operations or MISO, are bit more problematic. Information operations can be very broad and deep, including a very wide range of offensive, defensive and exploitative actions[216] of any computer systems discovered in the employment by Noordin's members, well as any systems in use by the organizations that share members or mechanisms with Noordin's network. Exploitation of Noordin's technical systems (i.e., via the Internet) augments the interference of the social systems via other means. No sovereign nation desires the U.S. to conduct information operations against it citizens. This is one instance of where the U.S. military may have to work with and through the Indonesian armed forces and domestic security apparatus to implement an effective information campaign in support of the overall strategy against Noordin.

Here, also, is an instance where a non-attributable third party could act on our behalf, wittingly or unwittingly, to inject harmful truthful information or misinformation into the social environment. Deception and deniability is critical to outside influence into the affairs of another society. In network terms, there would be a filter of structural holes and gate keepers whom no unwelcome probe could pass or circumvent. Again, this is a political choice filled with risk due to enormous uncertainty and high costs. But, it can be done.

10. Resources Available

Question 7. Are the necessary resources and personnel mobilized or available for action?

This question is answered in three parts. First, in practical terms for this environment, the question is a matter of international and interagency coordination and synchronization. For this reason, governments implement policy and priorities for such large and complex problems by designating a task force specially composed of appropriate agency representation, empowered and resourced appropriately for the work required. Those high-level governmental mechanisms are beyond the scope of this thesis, but the second part of this issue is core to the methodology described and must be understood by all levels of such a task force.

The second part of making resources available is answered by synchronization of efforts across the range of strategic options. Most of the people and tools necessary to defeat a network such as Noordin's and within Indonesia are not members of the U.S. government and must be either provided by the Indonesian government or recruited into the operation.

The final part of the mobilization discussion is that there are oftentimes grass-roots organizations or loosely-affiliated groups already doing the work, but not in a synchronized or coordinated manner. This may be desirable for the aspects of a campaign that involve exponentially larger efforts than targeting, such as institution building or reintegration and rehabilitation programs. One such example is the Singaporean community-based initiatives.[217] A government or other entity may be able to mobilize, fund and synchronize such groups that enables a greater impact through concentration of efforts and resources.

E. A STRATEGY FOR ATTACKING NOORDIN'S NETWORK

Our answers to the intervention decision tree questions, derived by following the Special Operations Target Network Analysis Process, bring us to a conclusion that there are multiple ways and means to disrupt, degrade and intervene against Noordin's terror network both in the short and the long term. I propose that our desired ends are not achieved by a silver bullet tactic or weapon, but would be best achieved by a symphony of complimentary intervention methods and tools that would bring about a tipping point[218] by creating vulnerabilities or exploiting those that already exist. Thus, the strategy I propose is not to employ a single strategy or a few of the strategies described by Roberts and Everton, but a strategy of simultaneous lines of effort across most or all of those categories of action resulting in a combination of subversion of the network itself and of poisoning the network neighborhood against it.

Illustrated in a model derived from Dr. Gordon McCormick's diamond model of counterinsurgency,[219] the overall strategy is one that pits the U.S. and Indonesian governments against Noordin's network using the Indonesian government-supportive portion of the Indonesian society to positively influence the non-supportive portion (Noordin's support base) to peel it away from Noordin's ideological draw (and that of other Islamic jihadist groups) simultaneously attacking the network directly whenever doing so will degrade the internal health of the network. The overall intent is to isolate and betray Noordin and his co-conspirators to the Indonesian authorities.

Using the framework illustrated in Figure 43, the chosen strategy requires bi-lateral actions and access to resources using U.S. and Indonesian strengths in a complimentary fashion. While some actions may be direct and provide immediate feedback, such as the kinetic targeting and law enforcement actions, some activities will require levels of Indonesian political and social consensus that endure for years. Those areas include improved protection of those soft targets known for their appeal to Islamic terrorist attacks, rehabilitation and reintegration through effective prison reform, community policing and local governance development. Executed and funded properly, and with a sensitivity to cultural realities, these efforts ought to have the cumulative effect of moving the Indonesian government toward solutions in the two essential mutually-reinforcing problems of local governance reform and an especially violent jihadist terror organization operating within Indonesian territory. Thus, we address those two problems coherently: attack the network directly via kinetic and non-kinetic methods, and attack it indirectly by non-kinetic methods that reshape the social environment to isolate Noordin and improve Indonesia's ability to govern in social sectors that provide support to him.

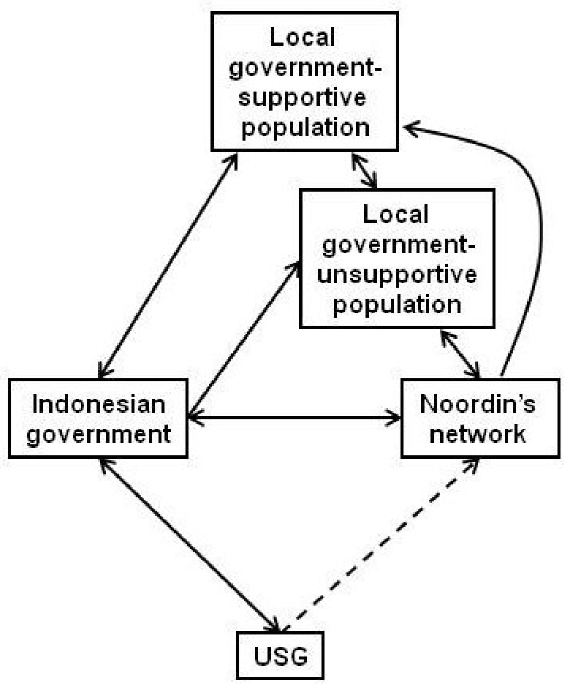

Figure 43. A model of a basic strategy to intervene against Noordin's network. The dashed line between the U.S. Government (USG) and Noordin indicates the relatively limited manner in which the USG can directly attack or influence Noordin's network.

To detail the strategy, Figure 44 depicts the several lines of effort necessary to holistically achieve the desired effects. There are several efforts that must occur simultaneously as they are complementary. Some efforts are successive and contingent upon previous actions. One such example is the actions involving development of intelligence collection within the local-government-unsupportive portion of the Indonesian population. Significant to this thesis, another example is the spotting, assessing, development and employment of former prison inmates associated with Noordin's network, or groups or individuals closely associated with him, as "pseudo gang" members to infiltrate into their former jihadist organization to collect and report information about key leader actions and intentions. After a brief description of the general strategy, a detailed section on the advantages of SONAP as applied to pseudo operations follows and concludes this chapter.

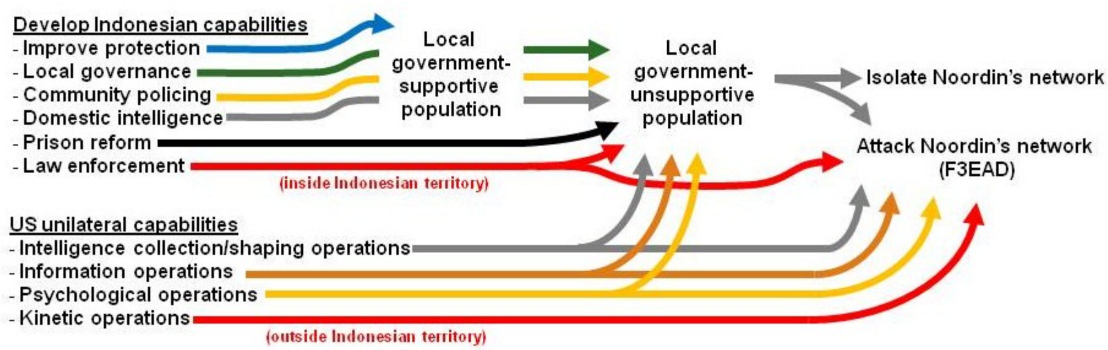

Figure 44. An overall strategy for attacking Noordin's network. The arrows of like colors represent bilateral lines of effort that require synchronization and complementary actions and resources. All efforts should be synchronized and complimentary.

1. Indirect and Direct Components of the Strategy

The indirect component is intended to re-shape the pool of society that is sympathetic to violent jihad. Re-shaping the social environment and influencing Noordin's network neighborhood includes prison reform, better governance in the jihad-sympathetic portion of the Indonesian population, better protecting the friendly sectors of Indonesian society via community policing, and target hardening. Working with and through local communities for governance assistance in building institutions capable of countering violent jihadist appeal is also useful. These macro-level changes are difficult to measure, so we must focus on a smaller, more measurable scale. Here, we look inside Noordin's network at the health of the organization itself.

The direct component of the strategy is to attack the network by employing PsyOp, IO, and U.S.-assisted Indonesian kinetic operations supported by development of their own CT capabilities and technological and human capacity of modern counter-terror methods. Employing F3EAD will involve getting inside Noordin's network's information cycles and, here, literally inside his organization. These functions are informed by intelligence operations, or sustained deliberate actions to collect defined and measurable information.

The Indonesian government requires early warning of impending attacks at the very least, if not some form of predictive analysis of where key players will be and when and in what posture. They may even choose to create a rapid reaction capability to react to warnings and prevent attacks or through which to attack the network itself. We also need to be able to measure the effects of the other lines of effort upon the health of the organization. Simply measuring the frequency or lack of attacks is a poor measurement of success, and is more an expression of Noordin's successes at the micro level. Inside the organization, trust is the lifeblood through which members live and die. To that end, we will pry open the organization through the holes created by attrition and slip inside. We will infiltrate the sanctuary and weapons procurement mechanisms by investing in a specific set of relationships, starting with targeted individuals within the prison population who may be turned against their former comrades. We seek former criminals or insurgents who would be willing and able to effectively work for the other side.

This is achieved through a series of rehabilitation and reintegration programs which are already necessary for de-radicalizing the Indonesian prison population. With passive supervision and constant mentorship from a trusted confidant, the targeted individual(s) sway from their previous jihadist path to one of reconciliation and, perhaps, one enacting their renewed loyalty by assisting their country's law enforcement and counterterrorism efforts against their former co-conspirators. The most promising prospects are selected for recruitment and very special training. One method of employing them is in a complex and highly sensitive intelligence activity known as pseudo operations.

2. Pseudo Operations or Mechanism Replacement Operations

Pseudo operations are employment of individuals or small teams of government-supported or government-friendly agents feigning as insurgents, normally along with bona fide insurgent defectors, infiltrate enemy insurgent groups for purposes of intelligence collection or direct action raids for kill or capture missions, or both. Historically, these are predominantly intelligence operations supporting targeting or conducted by special operations components of national law enforcement agencies.[220]

For our purposes here, pseudo operations are inherently exploitative of structural holes in dark networks, and are especially attracted to regions or nodes of structural equivalence surrounded by structural holes. This is particularly true for missions that seek replacement of or brokerage between Key Player nodes. If pseudo teams are not trying to inject their own information into the network, then they are taking advantage of a lack of brokerage or Simmelian ties in order to disrupt the overall workings of the network. In SONAP concept terms, pseudo operations are individual or segmental mechanism replacement strategies for any purpose necessary—intelligence monitoring, influence or elimination of threat nodes, cells or mechanisms. The more embedded a node is, the better to replace it with a pseudo team or agent. Then the effects will be felt across a broader portion of the network and the team will be more aware of information across the network. Embeddedness is a social network perspective of access and placement, and pseudo operations seek to maximize it.

Pseudo operations have a checkered history of strategic effectiveness against insurgents, where foreign or other military forces of dissimilar ethnic composition may infiltrate an enemy force or group to collect intelligence or to conduct attacks with intimate knowledge of enemy locations, plans, force composition and strength. This is mostly due to the fact that most counterinsurgency campaigns are slow to emerge as political priorities and most military or intelligence operations subsequently arise quickly with much experimentation. Significant uses of pseudo forces were most notably by the British in Kenya against the Mau Mau (1952–60) and in Malaya (1948–60) against the ethnic Chinese communist insurgents, by the white Rhodesian military in the Rhodesian bush war against ZANLA and ZIPRA communist insurgents (1964–79) and by the

French in Algeria in the late 1950s' "Battle of Algiers."[221] The Selous Scouts were employed to great advantage both internally and outside of Rhodesia's borders, but strategic results were mixed.[222]

Advantages to effective pseudo operations are three-fold. Included are, 1) extremely accurate and timely intelligence due to uniquely powerful access and placement, 2) a general ability to affect situations in a timely manner due to being on-site and 3) even when one or more teams are compromised or insurgents suspect their existence, trust can be eroded or destroyed between real insurgent or terrorist groups because they do not know who they are dealing with. In our situation with Noordin's network, timing is important because Noordin is reconstructing his network right now. If we get our pseudo teams recruited, developed and deployed soon, then we can infiltrate his network as he hastens to call upon his weak ties to reconstruct his operative mechanisms and access to critical resources.

3. Lessons of Past Pseudo Operations

Although there were governments that benefited from pseudo operations, there was usually a high political cost when actions and effects were not controlled as well as they could have been. Learning lessons from these experiences is key to ensuring success in Indonesia. Read these lessons learned with an eye toward Roberts' and Everton's typologies of strategic choices of counterterrorism methods:

1. *Money counts*. Money incentivizes and rewards, but must be used discriminately and in tune with other cultural mores. For the pseudo gang member, the risk must be worth it.

2. *Alternatives to participation can be dire*. While money can incentivize, there must be a severe punishment that is known to all and is an effective deterrent to re-defecting back to the terror network.

3. *Coordination is critical*. The agency employing pseudo teams must strike a balance between synchronization of information across agencies and military units to ensure the safety of the teams and other friendly units, and security of information to prevent unwanted disclosures that could lead to team compromises and loss of access and placement.

4. *Successful pseudo operations depend upon response forces*. If a pseudo team has time-sensitive information, conventional military forces or law enforcement agencies need to be able to react quickly and efficiently. In this light, a special unit may have to be designated or created that is responsible for effective reactions to pseudo team alerts.

5. *Breaking enemy communications is key*. Effective centralized communications and control of members is bad for pseudo team operations. Pseudo teams rely upon a certain level of anonymity in order to operate within the ambiguity and uncertainty of dark networks. If Noordin maintains a very high centrality measurement throughout his reconstruction period, that could mean extreme difficulty in inserting a pseudo team into that high-trust environment. The bona fides used to introduce a team under such circumstances must be very, very strong and have plenty of backstop. For this strategy to work, the CT forces must breach enemy communications via IO and the pseudo team members must be embedded with the necessary jihadist organizations that will provide effective back-story.

6. *"Turned" terrorists are critical*. Any familiarity with the internal insurgent or terrorist environment—key people, locations, processes, or language—is an important asset that cannot be overlooked. A turned terrorist is valuable both deployed in the field and as an information source concerning the internal network environment. This can be as simple as knowing names and descriptions of network members, to knowing the secret passwords and procedures for verifying identification and the latest ideological talking points. The better-disciplined regions of Noordin's networks will be more difficult to penetrate because of the history of trusted relations used by Noordin and his core members. [223]

It is apparent that these lessons in pseudo operations are not confined to the military sphere. There are points to be made in most categories of action in Roberts' and Everton's typologies of strategic choices concerning counterterrorism. As these pseudo operations begin, several supporting campaigns must already be underway. The effects of each must be complementary, as successful pseudo operations cannot exist without effective recruitment of turned terrorists or supporters, and terrorists or their supporters cannot be turned without effective reconciliation. Effective reconciliation begins with an effective prison system and follow-on social systems to continue the re-integration process, which in Indonesia must be reformed.

Targeting the sanctuary and weapons procurement mechanisms for infiltration by our pseudo teams, we look to the current field of incarcerated members. There are two categories of pseudo members for our purposes here. First is the key informant, the man or woman who can give us insight into key functions, identities and locations and may not be suitable for deployment as a pseudo team member for infiltration back into their old network. Second is the deployable pseudo agent or pseudo team member. This is a man or woman who was previously close to the key informant, perhaps structurally equivalent, was of lesser status in the network, but knows at least some of the same people and can provide valid bona fides to speak with active members and gain their trust for the remainder of his pseudo team.

4. Detailed Analysis for Infiltration Access and Placement

There are two fields of measurements for success in the SONAP model: those directly impacting the network's and pseudo teams' status, and those indirectly impacting that status.* Initial and direct measurements of success are recruitment (wide acceptance of the pseudo team as part of the group), activation (initial requests or demands for support from them), promotion of the pseudo team leader to a higher status in the group, and reinforcement or operational expansion putting the pseudo team at the core of the larger mechanism or multiple mechanisms. This positive elevation of the status of the pseudo team can be characterized by measurable increases in direct relations to other network members

The best candidate for a pseudo team member with access and placement near Dharmawan is Ubeid. While he was merely a courier in his prior operational time, he has the proper academic credentials: he is an Ngruki, Darusyahadah, and An-Nur graduate. He is in his twenties and from Ngawi, East Java. He is a JI member and Mindanao veteran. He is fluent in Arabic. He was arrested in July 2004 and sentenced to three and a half years in May 2005. Therefore, his release time permits ample preparation and

* Refer to Chapter V, Figure 26 for the network status graphic.

training time. What makes his contribution the strongest is his enormous 2-degree reach across the network (see Figure 45) that also includes much of the main component of the residual 2006 network.

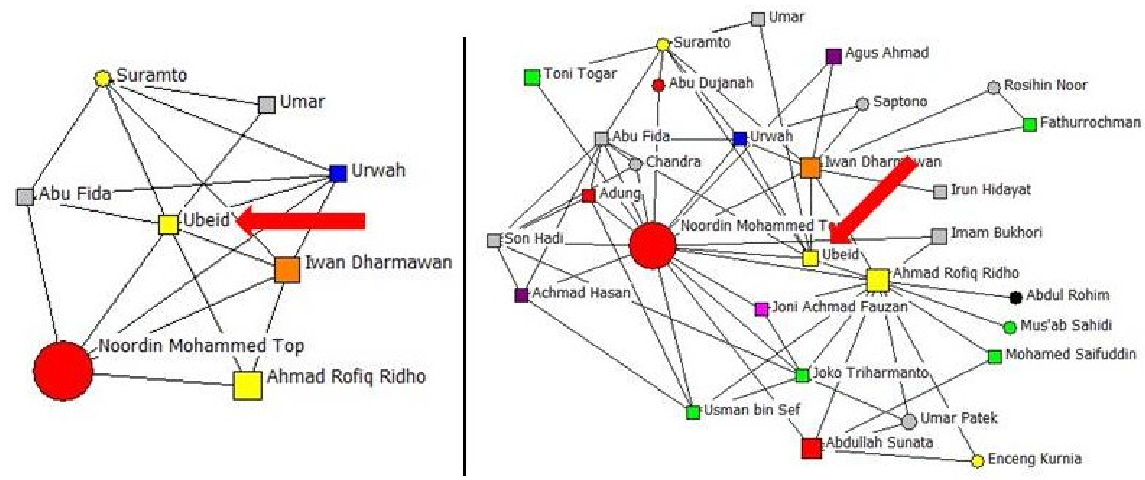

Figure 45. Ubeid's egonet (left) and 2-degree egonet (right). Reinsertion into the network could be validated by Suramto. Box-shaped nodes represent incarcerated members, circle-shaped nodes represent members still at large in 2006.

While no one can come close to replicating Noordin's 40% 1-degree reach across the network, Ubeid comes close with his 2-degree reach, and most (more than 50%) of those members are 1-degree away from Noordin. This makes him a significant source of information (within the jailed population, at least) of Noordin's core members' descriptions, intentions, and life patterns. After making contact with the network via Suramto, perhaps he can fulfill expectations in his new role as the sanctuary chief, or at least as a safe house network manager.

The next-strongest candidate to Ubeid for sanctuary mechanism infiltration is Bagus Budi Pranoto (aka Urwah) (see Figure 46). He is an Indonesian recruiter with distinction: he helped bring Iwan Dharmawan on board for the Noordin-led embassy bombing operation in 2004. He attended al-Mutaqien, Jepara, Universitas an-Nur, which means he has more than one layer of educational commonality with many prominent figures in the organization. After being detained, he was sentenced to three and a half years, in May 2005. Just as with Ubeid, if selected, his sentence would only have to be slightly abbreviated, if preparation and training permits. Urwah's possible points of contact for re-establishing relations with the network are Suramto and Saptono.

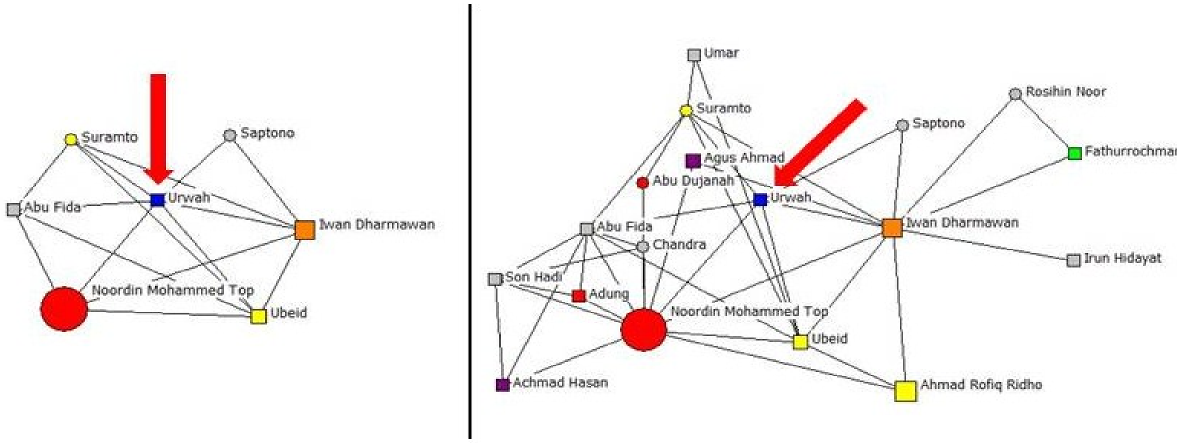

Figure 46. Urwah's egonet (left) and 2-degree egonet (right). Suramto and Saptono are his at-large contacts within the network.

In terms of resourcing mechanism/weapons procurement pseudo team member options, there are two potential pseudo team leaders, each with direct ties to Noordin and a small group of relations both at large and in jail: Abdullah Sunata and Ahmad Rofiq Ridho. In depth analysis of each of these men reveals significant opportunities and drawbacks.

First, there are some commonalities worth discussing: each of the men has 3–4 surviving acquaintances still at large. These men could possibly provide a form of bona fides and a path for re-contacting Noordin. Unfortunately, neither man has any relations still at large that also have a direct relationship with Noordin; this would be a much better form of bona fides once the pseudo team is employed. Another commonality is that each has a good group of facilitators and couriers. This is important because these roles include enough diverse tasks and activities that there is ample uncontrollable ambiguity for extra-organizational contacts (i.e.: an undercover handler or other government agent, or a choice of venues in which to introduce a pseudo team). In short, each man presents his own possibilities and risks.

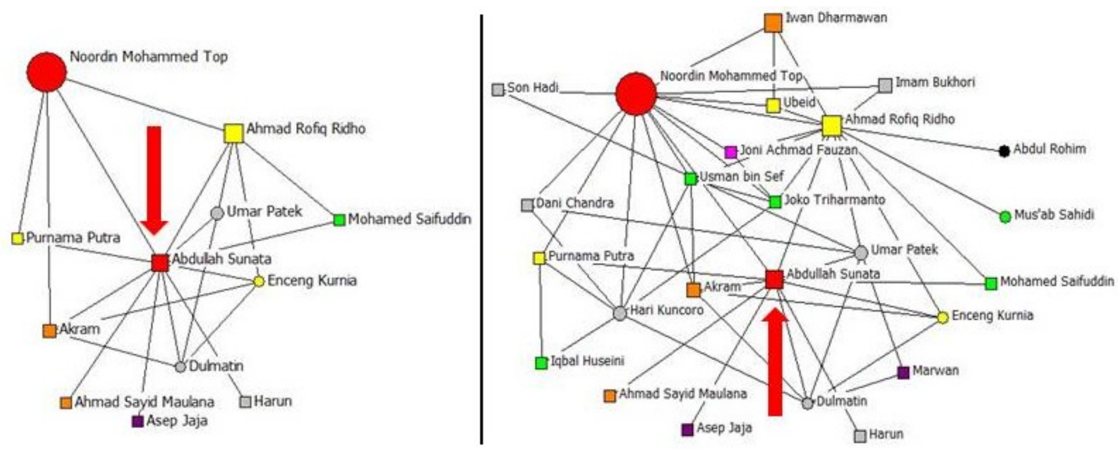

Figure 47. Abdullah Sunata's egonet (left) and 2-degree egonet (right). As with all the candidates, Sunata exhibits a moderate degree centrality and eigenvector centrality.

Abdullah Sunata (Figure 47) is Indonesian and was head of the KOMPAK office in Ambon from 2000–2001. After his arrest, he was sentenced to seven years in prison in April 2006 for withholding information about Noordin's whereabouts and additionally charged with illegal possession of weapons. Ironically, Noordin tried to get him to join forces in 2004, but he refused. This last fact may be key in opening Sunata to cooperating with us. Sunata has several options for re-establishing contact with the network: Dulmatin, Enceng Kurnia, or Umar Patek.

Ahmad Rofiq Ridho (Figure 48) is Indonesian and was a courier for Noordin in 2004. He is a Ngruki alumnus which puts him in a higher class within the organization. He lost two relatives—his brother, Fathurrahman al-Ghozi, and cousin, Jabir, were killed. He has combat experience as a veteran of Ambon and he is a member of JI. He was arrested in July, 2005, and sentenced to seven years beginning in April 2006. He had access into the financing branch of the resourcing mechanism while he was active; he is one of only two currently surviving donations middlemen. Donations can come from anywhere, and the cover for his access to increased funding can be easily explained by contacts made within the prison system. This is an excellent way to disburse untraceable "mystery" funding via clandestine Indonesian or USG accounts and cash hand-overs. Ridho also has several options for re-contacting the network as well as a couple of isolates: Umar Patek and Enceng Kurnia are with the network and Abdul Rohinm and Mus'ab Sahidi are the isolates.

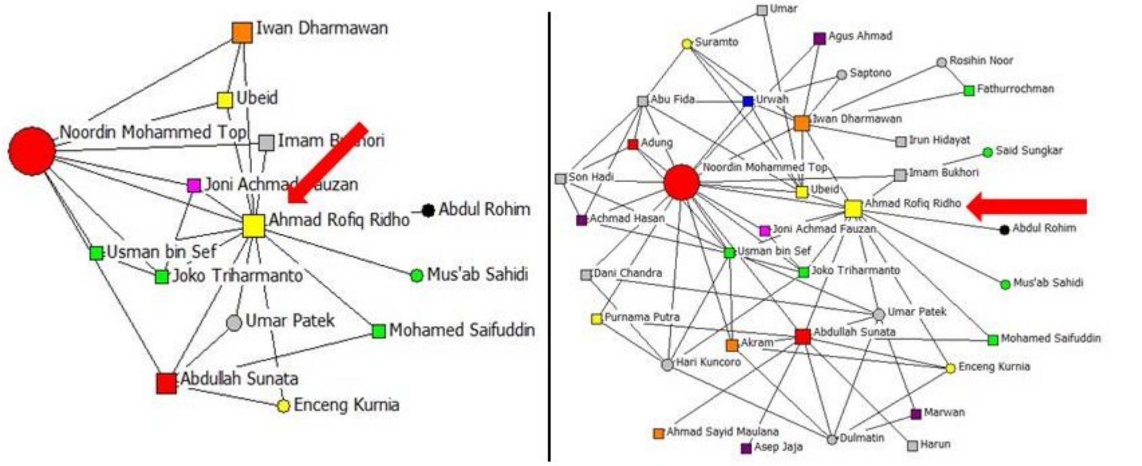

Figure 48. Ahmad Rofiq Ridho's egonet (left) and 2-degree egonet (right). Re-introducing Ridho to the network, but as a turned pseudo team member, could be a significant accomplishment.

These pseudo team candidates will become members of a largely Indonesian intelligence or law enforcement-run pseudo operation, conducted with U.S. assistance. The larger operation surrounding the pseudo teams involves much more than the aforementioned prison and reintegration processes. In order for these teams to become established in their cover stories and roles, there must be two dynamics in play, regardless of which mechanisms they are infiltrating. First, their own stories and resources must check out under scrutiny, the weak ties to the schools, for example, must be made apparent. Information operations must support them by providing technological back-story and advantages over teams' competitors—other groups in the same market as they are, so to speak. If there are other weapons providers, for example, then they must be raided by law enforcement, or put out of business, underbid, suspected of collaboration or otherwise discredited. There can be an air of suspicion built around their Internet presence whether it is missing or false emails, bank errors that suddenly drain funds or otherwise draw unwanted attention of authorities or other network members.

Second, and more to the indirect approach, psychological operations and positive influences from institution building and prison reform (mainly de-radicalizing integrative and rehabilitative programs) must begin to poison the network's environment. This should have the dual effects of reducing the pool of resources as well as increasing the perceptions of good governance. Where the more direct approach makes things easier for our teams to operate, these and other non-kinetic methods are designed to make things harder for the dark networks to operate. Only through this two-pronged approach can Indonesia reduce the threat from jihadist terrorism.

In the manner described here, the Special Operations Network Analysis Process can directly contribute to implementation of a multi-lateral approach to countering terrorism. Understanding a targeted dark network's internal and external structures assists in understanding the social systems which exist inside and outside the network's boundaries. Key to enabling a campaign of great scale and magnitude as this one is selecting tactics and techniques sufficient to collect the amount of information necessary from the right places—such as pseudo operations, information operations via the Internet, and exploiting the positive effects of prison reform (in this instance). Then, using established tools to understand the network mechanisms and how their structure allows them to exploit the surrounding social systems is critical to determining key players, key mechanisms, and measuring their vulnerabilities. Above all, embedding proper agents inside such systems is the most advantageous way to achieve inside information– turning on the light in a dark network, so to speak. Once we achieve proper access and placement, then we may measure the real impacts of all the other efforts applied to such a campaign and know when, where and how to act to keep the enemy off balance and vulnerable.

VII. CONCLUSIONS, POLICY IMPLICATIONS AND FUTURE WORK

Understanding and attacking terror and insurgent networks in the modern age requires a model that not only accounts for complexity in social networks, but also a strategy that takes advantage of social systems in the same manner that the terrorists do. All of the parties involved must make do with the tools and systems they have, and collaboration between parties is vital for success. Each party moves freely in and takes full advantage of the social networks that are most like them, they infiltrate and exploit the social structures that constitute contested human terrain, and attempt to intervene against key locations within those networks and systems that support or constitute the enemy. Using the Special Operations Network Assessment Process, or SONAP, informed by a systems understanding of social structures internal and external to a network under analysis, evaluates network member criticality, accessibility, role or function recuperability, and vulnerabilities of a particular location in a network, the effects of intervention at that location, and recognizability of specific members and positions in the network. The sum of the process can reveal the social structures of opportunities and risks for intervening against a dark network.

SONAP combines the Special Forces CARVER target analysis tool with several concepts from SNA to produce a method to estimate dark network structural patterns and properties and measure structural changes. The six factors in CARVER analysis have some close analogs within SNA, which make some of the SONAP combinations a rather natural fit. Some SNA concepts play a strong role in identifying mechanisms and other structures with CARVER, such as structural holes, centrality and density. SONAP also offers a range of intervention methods and approaches to maximize the structural and cognitive degradation of a dark network, as well as a way to measure the structural effects of intervention or other influences upon the network.

The implications of developing and implementing SONAP for military special operations forces, law enforcement and intelligence agencies are enormous. The conventional U.S. military has not embraced SNA as a tool—nor accepted the human domain as a valid concept—and is therefore unable to implement SONAP. For years, the

U.S. military and intelligence agencies have disaggregated terror, insurgent or resistance organizations into sub-groups by attributes, ignoring social relational data. In so doing, we have missed significant opportunities to understand social networks, especially when trying to intervene against dark networks in places such as Iraq and Afghanistan. Tools like SONAP can help overcome our methodological shortfalls and illustrate to us the mechanisms and patterns of dark networks.

A high level of competence in using a systemic approach, like SONAP, in understanding terror networks and the social systems in which they move can lead to increasingly efficient processes of intervening through the human terrain. There is nothing revolutionary about SONAP. It is composed of existing theories and established practices arranged in an order that assists in selecting methods to reach key players in critical social structures within a targeted network. Especially in the Internet age, everything about SONAP is accessible to any agency concerned with violent groups that exploit weakly-controlled social spaces. Only the technologies, authorities and funding allowed by law will limit the depth and breadth of any investigation and intervention strategy implementation.

The conceptual work is not finished, however, and the opportunities for practical applications are deep and wide and as varied as there is the funding and will to experiment. There are several areas that could use more research and validation. First, SNA as a family of concepts and tools is still wide open for experimentation and full of pitfalls.[224] And the most severe factor in analyzing dark networks is trying to account for the unknown amounts of missing data—the undiscovered artifacts of dark networks. Data collection of dark network social relations is problematic at best, and the work of SNA in general—while technical—is very much an art to be explored with alternative hypotheses and analyses being the rule rather than exception.

Second, the analytical model must be usable at all levels of analysis. Contrary to the 2006 dataset used here to explore these concepts, the real world is not static and evolves simultaneously strategically and tactically, and at varying speeds. SNA tools must be adaptable to real-time information as it becomes available and be able to display modified or alternative outcomes to new information. While this is not necessary for designing entire military or counterterrorism campaigns, it is necessary for tactical- and operational-level intelligence analysis and mission planning. The methods of collection, reporting, synthesis and display need to at least keep pace with the speed of today's counterterrorism operations. For the slow-motion strategic unfolding of unconventional warfare or foreign internal defense campaigns (such as counterinsurgencies), the value of SONAP will be in the common language used and broad range of analysis made possible as applied from the tactical to the strategic levels of analysis and planning. The value of a common language for articulating analysis in every domain and at every level is inestimable.

Lastly, the biggest challenge for implementing tools such as SONAP is the flexibility and adaptability of the organizations that need it. Within organizations charged with intervening in irregular warfare environments, the analysts, operators, commanders, and their tools need to be able to understand and support the emergent creative destruction that their missions require. And they need to be able to incorporate new ideas and methods rapidly. This organizational adaptability and flexibility is why SOF are capable of incorporating SONAP into their arsenal. The concerns reach into the most important aspects of an organization: leadership, management, organizational patterns and internal systems and processes. Above all, the leadership must be comfortable with ambiguity and uncertainty in their decision making. The scope and scale of the complexity at all levels demand maximal organizational adaptation not just conceptually, but practically as well. After all is said and done, in ambiguous and uncertain irregular warfare domains like counterinsurgency, counterterrorism and unconventional warfare, organizations adapt or die.

THIS PAGE INTENTIONALLY LEFT BLANK

NOTES

[1] David Gurteen, "On defining the problem by Albert Einstein," accessed June 25, 2010, http://www.gurteen.com/gurteen/gurteen.nsf/id/L004680/.

[2] Sir Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (London: Penguin, 2005), 17–18.

[3] James Roseneau, "Many Damn Things Simultaneously," (a paper presented at the Conference on Complexity, Global Politics, and National Security, sponsored by the National Defense University and the RAND Corporation, Washington, D.C., November 13, 1996), http://www.dodccrp.org/html4/bibliography/comch04.html.

[4] Doug McAdam, *Political Process and the Development of Black Insurgency, 1930–1970* (Chicago: University of Chicago Press, 1999).

[5] Smith, *The Utility of Force: The Art of War in the Modern World*, 177–178.

[6] Jorg Raab and H. Brinton Milward, "Dark Networks as Problems," *Journal of Public Administration Research and Theory* 13 (2003) 413–439, doi: 10.1093/jopart/mug029.

[7] Smith, *The Utility of Force: The Art of War in the Modern World*, 199.

[8] Kimberly Dozier, "Petraeus Highlights Special Ops Successes in Afghanistan," *The Associated Press*, September 4, 2010, http://fayobserver.com/articles/2010/09/04/1027918?sac=Mil; Kimberly Dozier, "Green Beret Equals Special Forces—Got it?," *The Associated Press*, November 17, 2011, http://www.boston.com/news/nation/washington/articles/2011/11/17/special_forces_equals_green_berets_got_it/; Lisa Burgess, "Iraq War: Special Forces Followed up on Afghanistan Success," *Stars and Stripes*, May 27, 2003, http://www.stripes.com/news/iraq-war-special-forces-followed-up-on-afghanistan-success-1.6044.

[9] John Arquilla and David Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), 319.

[10] Department of Defense, *JP 2–01.3 Joint Intelligence Preparation of the Operational Evironment* (Washington, D.C.: GPO, 2009), I-3–I-5, II-44–II-78.

[11] John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago: Ivan R. Dee Publishing, 2008), 25–28, 156–181.

[12] Ken Tovo, "From the Ashes of the Phoenix: Lessons for Contemporary Counterinsurgency Operations," in *Special Warfare*, Vol 20, Issue 1 (U.S. Army JFK Special Warfare Center, Fort Bragg, NC, 2007), 7–15.

[13] Richard Hunt, "The Challenge of Counterinsurgency," in *Second Indochina War Symposium: Papers and Commentary*, edited by John Schlicht (Washington, D.C., GPO, 1986), 132–137.

[14] Ty Connet and Bob Cassidy, "VSO: More Than Village Defense," in *Special Warfare*, Vol. 24, Issue 3 (2011), 22–27.

[15] Hy Rothstein, *Afghanistan and the Troubled Future of Unconventional Warfare* (Annapolis, MD, Naval Institute Press, 2006), 96–102; Andrew F. Krepinevich, *The Army and Vietnam* (Baltimore, MD: Johns Hopkins University Press, 1986), 165.

[16] U.S. Library of Congress, Congressional Research Service, *Instances of Use of United States Armed Forces Abroad*, 1798–2007, by Richard F. Grimmett, CRS Report for Congress, RL32170 (Washington, DC: Congressional Information and Publishing, January14, 2008).

[17] Stockholm International Peace Research Institute, *SIPRI Yearbook 2008: Armaments, Disarmament and International Security* (Stockholm: Stockholm International Peace Research Institute, 2008). http://yearbook2008.sipri.org/files/SIPRIYB08summary.pdf. The SIPRI report covers four conventional conflicts in Eritrea-Ethiopia, 1998–2000;in India-Pakistan, 1998–2003; and the U.S./coalition-Iraq, 2003 and the 2008 Russian invasion of Georgia to secure the ethnic Russian enclaves of Abkhazia and South Ossetia.

[18] Angel Rabasa, et al., *Ungoverned Territories: Understanding and Reducing Terrorism Risks*, RAND Project Air Force, Report MG-561-AF (Santa Monica, CA: RAND, 2007), xv–xix, http://www.rand.org/pubs/monographs/2007/RAND_MG561.pdf; Robert D. Lamb, *Ungoverned Areas and Threats from Safe Havens: Final Report of the Ungoverned Areas Project*, (Washington, D.C.: GPO, 2007), 23–27.

[19] David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, D.C.: GPO, 2003)4–7.

[20] Of the many authors referred, advocates for doctrine driving technological change are: Williamson R. Murray and Allan R. Millett, *Military Innovation in the Interwar Period*, (New York: Cambridge University Press, 1996); and Stephen Rosen, *Winning the Next War: Innovation and the Modern Military*, (New York: Cornell University Press, 1991). The authors proposing that technological innovation precedes and influences doctrinal shifts are: Robert L. O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression* (New York: Oxford University Press, 1989); William McNeill, *The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000*, (Chicago: University of Chicago Press, 1984).

[21] Roseneau, "Many Damn Things Simultaneously: Complexity Theory and World Affairs,"1996, 1–3.

[22] Arquilla and Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy,* 6–7.

[23] For a militarily-useful discussion of complexity, see Roseneau, "Many Damn Things Simultaneously: Complexity Theory and World Affairs," 84–87.

[24] Laszlo Barabasi and Eric Bonabeau, "Scale-Free Networks," *Scientific American* (May, 2003), 53, http://www.nd.edu/~networks/Publication%20Categories/01%20Review%20Articles/ScaleFree_Scientific%20Ameri%20288,%2060–69%20(2003).pdf.

[25] James Moffat, *Complexity Theory and Network Centric Warfare* (Washington, D.C.: CCRP, 2003), xi.

[26] Ibid., xiii.

[27] Arquilla and Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, 317.

[28] Robert A. Hanneman and Mark Riddle, *Introduction to Social Network Methods* (Riverside, CA: University of California, 2005), http://faculty.ucr.edu/~hanneman/).

[29] Mark Granovetter, "Economic Action and Social Structure: The Problem of Embeddedness," *The American Journal of Sociology* 91, no. 3, (1985), 481–510, http://www.jstor.org/stable/2780199?origin=JSTOR-pdf.

[30] Martin Kilduff and Wenpin Tsai, *Social Networks and Organizations* (London: SAGE, 2003), 26–27.

[31] Anna lee Saxenian, *Regional Advantage: Culture and Competition in Silicon Valley and Route 128* (Cambridge, MA: Harvard University Press, 1994), 97.

[32] In order to maintain the lowest level of classification possible for this thesis, I eliminated all classified references and made maximal use of older and unclassified sources of information. For example, I do not use or describe the methodologies as delineated in the 2007 versions of FM 3–05.20 Special Forces Operations, FM 3–05.201 Special Forces Unconventional Warfare or other manuals, rather, I used conceptually similar but distinctively different sources so as not to compromise modern developments in SF doctrine. In some cases, I used the older, unclassified editions of manuals as reference when they were not remarkably different from their classified version. In those last, unreferenced manuals, it suffices to say that there is no further inclusion of complexity or SNA theoretical or practical applications.

[33] For those unaccustomed to military manuals, unlike their civilian academic counterparts, military manuals and doctrinal publications are assumed to be cumulative in their present editions. They are intended to be holistic and mutually supporting documents with references to supporting documents, also assumed to be holistic in their latest edition. New editions are usually revisions of previous versions that supersede the previous. The only military doctrinal publications to break from this model have been the Army and Marine Corps' 2006 version of the Counterinsurgency manual, its joint publication counterpart, JP 3–24, and TRADOC Pamphlet 525–500.

[34] Department of Defense, *JP 3–05.2 Joint Tactics, Techniques and Procedures for Special Operations Targeting and Mission Planning*, (Washington, D.C.: GPO, 2003), A-1–A-2.

[35] Department of Defense, *JP 3–0 Joint Operations*, (Washington, D.C.: GPO, 2008), IV-4–IV-14; Department of Defense, *JP* 5–0 Joint Operation Planning, (Washington, D.C., GPO, 2006), IV-8–IV-19; Department of Defense, *JP 2–0 Joint Intelligence*, (Washington, D.C., GPO, 2000), IV-19–IV-24; Department of Defense, *JP 3–60 Joint Targeting*, (Washington, D.C., GPO, 2007).

[36] Granovetter, "Economic Action and Social Structure: The Problem of Embeddedness," 481–510.

[37] Department of Defense, *JP 5–0 Joint Operation Planning*, III-16–III-19.

[38] Department of the Army, *FM 3–05 Army Special Operations Forces*, (Washington, D.C.: GPO, 2006), 7–4–7–5.

[39] Department of Defense, *JP 3–0 Joint Operations*, IV-4–IV-12.

[40] Department of Defense, *JP 5–0 Joint Operation Planning*, IV-8–V-22.

[41] Department of the Army, *FM 3–05.201 Special Forces Unconventional Warfare (S/NF)*, (Washington, D.C.: GPO, 2007), 4–1–4–5; Department of the Army, *FM 3–24 Counterinsurgency*, 2006, A-5–A-6. Referenced portion of FM 3–05.201 is unclassified.

[42] Department of the Army, *TRADOC Pamphlet 525–5-500 Commander's Appreciation and Campaign Design*, (Washington, D.C.: GPO, 2008).

[43] Department of Defense, *Commander's Handbook for an Effects-Based Approach to Joint Operations* (Washington, D.C.: GPO, 2006).

[44] Ibid., II-2.

[45] Ibid., II-1–II-12.

[46]James N. Mattis, "U.S. JFCOM Commander's Guidance for Effects-based Operations." *Parameters*, (Washington, D.C.: GPO, 2008), 18–25, http://www.carlisle.army.mil/usawc/Parameters/Articles/08autumn/mattis.pdf.

[47] Tilghman, Andrew, "Gates to Close JFCOM, Cut Gen. Officer Billets," *The Marine Corps Times*, August 9, 2010, http://www.marinecorpstimes.com/news/2010/08/military_gates_cuts_080910w/ .

[48] Department of the Army, *FM 3–05.201 Special Forces Unconventional Warfare* , 4–12. Referenced portion of FM 3–05.201 is unclassified.

[49] Department of Defense, *JP 3–60 Joint Targeting*, II-4–II-6, C-6–C-7, D-1–D-9.

[50] Albert-Laszlo Barabasi, *Linked: How Everything is Connected* (New York: Plume, 2002).

[51] John H. Holland, *Hidden Order: How Adaptation Builds Complexity* (Cambridge, Perseus Books, 1995).

[52] Roger Lewin, *Complexity: Life at the Edge of Chaos* (New York: MacMillan Publishing Co, 1992).

[53] M. Mitchell Waldrop, *Complexity: Emerging Science at the Edge of Order and Chaos* (New York: Simon and Schuster, 1992).

[54] Moffat, *Complexity Theory and Network-Centric Warfare*.

[55] Edward Smith, *Complexity, Networking and Effects-Based Approaches* (Washington, D.C.: GPO, 2006).

[56] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network-Centric Warfare, (*Washington, D.C.: GPO, 1999).

[57] CCRP homepage, accessed April 15, 2008, http://www.dodccrp.org/html4/about_main.html.

[58] Arquilla and Ronfeldt, *Networks and Netwars*: *The Future of Terror, Crime, and Militancy*, 6.

[59] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin, 2006).

[60] Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology*, 78 (1973): 1360–1380, http://sociology.stanford.edu/people/mgranovetter/documents/granstrengthweakties.pdf.

[61] Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications* (Cambridge: Cambridge University Press, 1994).

[62] Georg Simmel, "Individual and Society," in K.H. Wolff, *The Sociology of Georg Simmel*.(New York: Free Press, 1950); Georg Simmel, "The Sociology of Secrecy and of the Secret Societies," *American Journal of Sociology* 11 (1906): 441–498.

[63] Ronald S. Burt, *Structural Holes: The Social Structure of Competition* (Cambridge, MA: Harvard University Press, 1992).

[64] Linton Freeman, “Centrality in Social Networks: Conceptual Clarification,” *Social Forces* 60 (1979): 215–239. http:// moreno.ss.uci.edu/27.pdf.

[65] Hanneman and Riddle, “Introduction to Social Network Methods,” (Riverside, CA: University of California, Riverside, 2005). http://faculty.ucr.edu/~hanneman/.

[66] Stephen Borgatti, Martin Everett, and Linton Freeman, *UCINET 6.0 Version 6.411* (Natick: Analytic Technologies, 1999); Stephen Borgatti, “Identifying Sets of Key Players in a Network.” *Computational & Mathematical Organization Theory* , April 2006: 21–34.

[67] John Scott, *Social Network Analysis: A Handbook,* 2nd ed. (Newberry Park, CA: Sage, 2000).

[68] Stephen Borgatti, *UCINET Software History,* https://sites.google.com/site/ucinetsoftware/history .

[69] Martin Kilduff and Wenpin Tsai, *Social Networks and Organizations*.

[70] Peter R. Monge and Noshir S. Contractor, *Theories of Communications Networks* (New York: Oxford University Press, 2003).

[71] Valdis Krebs, “Uncloaking Terrorist Networks,” *FirstMonday* 7(2002), http://firstmonday.org/issues/issue7_4/krebs/index.html.

[72] Georg Simmel, “The Sociology of Secrecy and of the Secret Societies,” 441–498.

[73] Lawrence E. Hazelrigg, “A Re-examination of Simmel’s ‘The Secret and the Secret Society’: Nine Propositions,” *Social Forces* 47 (1969): 323–330.

[74] Bonnie H. Erickson, “Secret Societies and Social Structure,” *Social Forces* 60 (1981): 188–211, http://www.jstor.org/stable/2577940.

[75] Malcom K. Sparrow, “The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects,” Social Networks 13 (1991): 251–274, http://ksgfaculty.harvard.edu/faculty/cv/MalcolmSparrow.pdf.

[76] Peter Klerks, “The Network Paradigm Applied to Criminal Organizations,” *Connections* 24 (2001): 53–65.

[77] Brian Reed, “A Social Network Approach to Understanding Insurgency,” *Parameters* (Summer, 2007), 19–30.

[78] Wayne E. Baker and Robert R. Faulkner, “The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry,” *American Sociological Review* 58 (1993): 837–860.

[79] Rabb and Milward, “Dark Networks as Problems,” 413–439.

[80] Jose A. Rodrigues, “The March 11th Terrorist Network: In its Weakness Lies its Strength” (working paper, Department of Sociology and Analysis of Organizations, University of Barcelona, 2005).

[81] Valdis Krebs, “Mapping Networks of Terrorist Cells,” 43–52.

[82] Stuart Koschade, “A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence,” *Studies in Conflict and Terrorism* 29 (2006) 559–575. http://www.safeguardingaustralia.org.au/files/Koschade_JI_article.pdf.

[83] Kathleen M. Carley and Yuqing Ren, "Tradeoffs Between Performance and Adaptability for C3I" (Interim paper, Pittsburgh: Carnegie Mellon University, 2001).

[84] Kathleen M. Carley, Ju-Sung Lee and David Krackhardt, "Destabilizing Networks," *Connections*, 2002: 79–92.

[85] Carley, Lee and Krackhardt, "Destabilizing Networks," 79–92; Matthew Dombroski, Paul Fischbeck, and Kathleen Carley, "Estimating Shape of Covert Networks," *Proceedings of the 8th International Command and Control Research and Technology Symposium*, Washington, DC. http://www.casos.cs.cmu.edu/publications/papers/dombroski_2003_estimatingshape.pdf (accessed April 15, 2007); Kathleen Carley, Jana Diesner, Jeffrey Reminga, Maksim Tsvetovat, "An Integrated Approach to the Collection and Analysis of Network Data," *Proceedings of the NAACSOS 2004 Conference*, http://www.casos.cs.cmu.edu/events/conferences/2004/2004_proceedings/Carley_Diesner_Reminga.pdf (accessed April 15, 2007); Kathleen Carley, Jeffrey Reminga and Steve Borgatti, "Destabilizing Dynamic Networks Under Conditions of Uncertainty," (paper presented at International Conference on Integration of Knowledge Intensive Multi-Agent Systems, 30 Sept.–4 Oct. 2003), 121–126, http://ieeexplore.ieee.org/iel5/8803/27847/01245033.pdf?arnumber=1245033; Kathleen Carley, "Dynamic Network Analysis for Counter-Terrorism," University of Illinois Urbana-Champagne, doi. 10.1.1.137.9475.

[86] Shishir Nagaraja and Ross Anderson, "Topology of Covert Conflict," University of Cambridge, Computer Laboratory Technical Reports, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-637.html (accessed April 15, 2007).

[87] Stephen P. Borgatti, "Identifying Key Sets of Players in a Social Network," *Computational Mathematics and Organizational Theory* 12 (2006), doi 10.1007/s10588–006–7084-x.

[88] Phillip Bonacich, "Technique for Anlayzing Overlapping Memberships," *Sociological Methodology* 4 (1972), 176–185. http://www.jstor.org/stable/pdfplus/270732.pdf.

[89] Phillip Bonacich, "Some Unique Properties of Eigenvector Centrality," *Social Networks* 29, no. 4 (2007), 555–564.

[90] Coralio Ballester, Antoni Calvo-Armengol, and Yves Zenou, "Who's Who in Crime Networks. Wanted: The Key Player," *Econometrica* 74 (2006), 1403–1417. http://users.eecs.northwestern.edu/~nickle/socNet/keyplayer.pdf.

[91] John Dodson, "Man-hunting, Nexus Topography, Dark Networks and Small Worlds," *IO Sphere* (Winter, 2006), pp. 7–10.

[92] Brian Reed, "A Social Network Approach to Understanding Insurgency," 19–30.

[93] Jonathan T. Hammill, "Analysis of Layered Social Networks" (PhD. Diss., Air Force Institute of Technology, 2006).

[94] Victoria Hougham, "Sociological Skills Used in Capture of Saddam Hussein," *Footnotes* http://www.asanet.org/footnotes/julyaugust05/fn3.html.

[95] Maksim Tsvetovat and Kathleen Carley, “Bouncing Back: Recovery of Mechanisms of Covert Networks,” (paper presented at NAACSOS Conference Proceedings Pittsburgh, PA, 2003). http://www.casos.cs.cmu.edu/publications/working_papers/tsvetovat_2003_recovery.pdf.

[96] Montgomery McFate, “Iraq: The Social Context of IEDs,” *Military Review* 85 (2005), 37–40.

[97] Scott Swanson, “Viral Targeting of the IED Social Network,” *Small Wars Journal* 8, (2007). http://smallwarsjournal.com/documents/swjmag/v8/swanson-swjvol8-excerpt.pdf.

[98] Elisa Jayne Bienensock and Phillip Bonacich, “Balancing Efficiency and Vulnerability in Social Networks,” (paper presented and collected in *Dynamic Social Network Modeling and Analysis: Workshop Papers*, 2003), 253–264. http://www/nap/edu/catalog/10735.html.

[99] Interestingly, the conflict between efficiency and security in SNA and secret society literature mirrors the conflict in U.S. Army Special Operations literature between synchronization and security as one of the so-called Special Operations Imperatives.

[100] Simson L. Garfinkel, “Leaderless Resistance Today,” *FirstMonday* 8 (2003). http://www.firstmonday.org/issues/issue8_3/garfinkel/#author.

[101] Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century*, (Philadelphia: University of Pennsylvania Press, 2008).

[102] Brafman and Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*.

[103] Louis Beam, “Leaderless Resistance,” *The Seditionist*, 12 (February 1992), 12–13. http://www.louisbeam.com/leaderless.htm, pp.

[104] Department of Defense, “Unifed Command Plan 2011.” *www.defense.gov*. 2011. http://www.defense.gov/home/features/2009/0109_unifiedcommand/.

[105] *Countering Violent Extremism Hearing Before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities*. 111th Cong., 2nd sess. (2010). (testimony of LTG Francis H. Kearny, III). March 10, 2010. armed-services.senate.gov/statemnt/2010/.../Kearney%2003–10–10.pdf (accessed April 15, 2011).

[106] Robinson, Linda. “Men on a Mission: U.S. Special Forces are Retooling for the War on Terror.” *www.usnews.com.* March 9, 2006. http://www.usnews.com/usnews/news/articles/060903/11shadow_print.htm.

[107] Department of Defense, *JP 5–0 Joint Operation Planning*, B-1.

[108] Vandenbrouke, Lucien. *Perilous Options: Special Operations as an Instrument of Foreign Policy*. (New York: Oxford University Press, 1993).

[109] Department of the Army, *Special Forces Qualification Course 18A Course Student Curriculum Handouts.* 1999.

[110] Department of Defense, *JP 3–05.2 Joint TTPs for Special Operations Targeting and Mission Planning*, A-1.

[111] Rowan Scarborough, “Special Operations Forces Eye Terrorists,” *The Washington Times.* Washington, D.C., August 11, 2005.

[112] Christopher J. Lamb, and Evan Munsing. *Secret Weapon: High-value Target Teams as an Organizational Innovation* (Washington, D.C.: NDU Press, 2011), 1.

[113] Department of Defense, *JP 3–0 Joint Operations* (Washington, D.C.: GPO 2011), V-32.

[114] Department of Defense, *JP 3–05.2 Joint Tactics, Techniques, and Procedures for Special Operations Targeting and Mission Planning*, II-2.

[115] Ibid., II-11, A-4–A-5.

[116] Department of Defense, *JP 3–0 Joint Operations* (Washington, D.C.: GPO, 2011), *xi–xii*.

[117] Department of the Army, *FM 3–05.20 Special Forces Operations*, 5–2–5–13.

[118] Some observers have argued that SOF have drifted toward conventional or hyper-conventional tactics and methods over the last several years of warfare. Organizations tend toward what gets rewarded in combat theaters; as in when SOF act in direct support to conventional force commanders, the senior command rewards the actions that best meet conventional expectations or demands, rather than performing tasks more appropriate to the form of warfare or the environment. This is not the intended methodology for SOF. See Hy Rothstein, *Afghanistan and the Troubled Future of Unconventional Warfare (*Annapolis: U.S. Naval Institute Press, 2005).

[119] Department of the Army, *FM 3–05 Army Special Operations Forces*, 1–13–1–15.

[120] Department of Defense, *JP 3–05.2 Joint TTPs for Special Operations Targeting and Mission Planning*, A-1–A-2.

[121] Ibid., II-12.

[122] Ibid., A-2–A-6.

[123] Ibid., A-5–A-6.

[124] Ibid., A-4.

[125] See note 124 above.

[126] See note 124 above.

[127] Ibid., II-10–II-16.

[128] James Moffat, *Complexity Theory and Network Centric Warfare*, 23–43, 57–74.

[129] This description of triangulation of data, as explained by Ms. Alexandra Courtney of USAID, is a taken from a Disarmament, Demobilization and Reintegration workshop held at the Naval Postgraduate School in Monterey, CA from 30 March–2 April, 2008.

[130] David Curtis, “How can we See Black Holes?” *Spacetime Wrinkles Exhibit* (1995), http://archive.ncsa.uiuc.edu/Cyberia/NumRel/BlackHoleHowSee.html (accessed April 26, 2008).

[131] Diagram created by the author. All images within are courtesy of Wikipedia's Wikimedia Commons (http://en.wikipedia.org/wiki/Hydroelectricity), non-attributable freeware/shareware (www.coolclips.com), or are the creation of the author. Retrieved April 20, 2008.

[132] Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications*, 6.

[133] Wouter De Nooy, Andrej Mrvar and Vladimir Batagelj, *Exploratory Social Network Analysis with Pajek*, (New York: Cambridge University Press, 2005), 5.

[134] Ibid., 29–57.

[135] Georg Simmel, "The Sociology of Secrecy and of Secret Societies," 441–498.

[136] Bonnie Erickson, "Secret Societies and Social Structure,." *Social Forces* 60 (1981): 188–210.

[137] Gilbert Herdt, "Secret Societies and Secret Collectives," *Oceania* 60, no. 4 (1990): 360–381.

[138] J. Bowyer Bell, *Dragonwars: Armed Struggle and the Conventions of Modern War* (London: Transaction Publishers, 1999), 155.

[139] Wasserman and Faust, *Social Network Analysis: Methods and Applications,* 31.

[140] Malcolm K. Sparrow, "The application of network analysis to criminal intelligence: An assessment of the prospects," *Social Networks*, 13, (1991), 251–274; Valdis E. Krebs, "Uncloaking Terrorist Networks,"). 1–2.

[141]John Scott, *Social Network Analysis: A Handbook*, 2–5.

[142] Discussions with a Special Forces Chief Warrant Officer 3 who acted as a SOTF and JSOTF Senior Targeting Officer in Iraq for four years in 2009, and a Chief Warrant Officer 4 who acted as senior targeting Officer for Multinational Corps-Iraq for one year in 2009.

[143] John Robb, *Brave New War* (Hoboken, NJ: John Wiley and Sons, Inc. 2007), 111–129.

[144] Ibid., 123–125.

[145] Conversations with military intelligence and special operations personnel, 2004–08. Timely awareness of such meetings or planning sessions has directly led to time-sensitive direct action missions to kill or capture insurgents and terrorists in Iraq, Afghanistan and other locations.

[146] Adapted from Wasserman and Faust, *Social Network Analysis: Methods and Explanations,* 241.

[147] Piotr Stompka, *Trust: A Sociological Theory*, (New York: Cambridge University Press: 1999), 25, and Burt, Ronald S. *Structural Holes: The Social Structure of Competition* (Cambridge: Harvard University Press, 1992), 15–16.

[148] David Krackhardt, "Simellian Ties: Super Strong and Sticky," in *Power and Influence in Organizations,* edited by Roderick Kramer and Margaret Neale, (Thousand Oaks, CA: Sage, 1998), 21–38.

[149] Mark Granovetter, "The Strength of Weak Ties," 1360–1380; Mark Granovetter, "The Strength of Weak Ties: A Network Theory Revisited," *Social Structure and Analysis,* edited by P. Marsden and N. Lin. (Bevery Hills, CA: Sage, 1982).

[150] Granovetter, “The Strength of Weak Ties,” 1350–1368.

[151] de Nooy, Mrvar, and Batagelj, *Exploratory Social Network Analysis with Pajek,* 151.

[152] Krackhardt, “Simellian Ties: Super Strong and Sticky,” 24.

[153] David Krackhardt, “The Ties That Torture: Simmelian Tie Analysis in Organizations,” *Research in the Sociology of Organizations* 16 (1999): 183–210.

[154] Burt, Ronald S. *Structural Holes: The Social Structure of Competition,* 1.

[155] Ibid., 13.

[156] Ibid., 25–30.

[157] Martin Kilduff and Wenpin Tsai, *Social Networks and Organizations,* 28.

[158] Scott, *Social Network Analysis: A Handbook,* 80.

[159] Borgatti, Stephen. “Identifying Sets of Key Players in a Network,” 21–34.

[160] Ibid., 21–22.

[161] Freeman, “Centrality in Social Networks: Conceptual Clarification,” 221.

[162] Scott, *Social Network Analysis: A Handbook*, 85.

[163] Freeman, “Centrality in Social Networks: Conceptual Clarification,” 215–239.

[164] Deone Zell, “Social Network Analysis and Knowledge Management,” www.d*ocstoc.com.* USC, Fairfield. April 28, 2007. http://www.docstoc.com/docs/81260581/Social-Network-Analysis (accessed April 15, 2010).

[165] Freeman, “Centrality in Social Networks Conceptual Clarification,” 224.

[166] M. E. J. Newman, “The Mathematics of Networks.” *www-personal.umich.edu.*, accessed August 20, 2009.www-personal.umich.edu/~mejn/papers/palgrave.pdf, 5.

[167] Peter Monge and Noshir Contractor, *Theories of Communications Networks*, 141–240.

[168] de Nooy, Mrvar, and Batagelj, *Exploratory Social Network Analysis with Pajek,* 44–148.

[169] Smith, *The Utility of Force: The Art of War in the Modern World*,18.

[170] Arquilla and Ronfeldt, “Netwar Revisited: The Fight for the Future Continues,” in *Networks, Terrorism and Global Insurgency*, edited by Robert J. Bunker, (New York: Routledge, 2006), 8–19.

[171] Michael Sullivan, *How to Win and Know It: An Effects-Based Approach to Irregular Warfare* (master’s thesis, Naval Postgraduate School, 2007).

[172] Sidney Tarrow, *Power in Movement: Social Movements and Contentious Politics,* 2nd edition (New York: Cambridge University Press, 1998), 123–138.

[173] Carley, Kathleen, Ju-Sung Lee, and David Krackhardt. “Destabilizing Networks.” 79–92.

[174] J. Bowyer Bell, *The Dynamics of the Armed Struggle* (London: Cass, 1998), 178.

[175] Walid Phares, *The War of Ideas (*New York: Palgrave Macmillan, 2008).

[176] Scott Mann,”The Shaping Coalition Forces’ Strategic Narrative in Support of Village Stability Operations.” *www.smallwarsjournal.com.* 2011. http://smallwarsjournal.com/blog/journal/docs-temp/721-mann.pdf.

[177] David Snow, E. Burke Rochford, Steven Worden, and Robert Benford, “Frame Alignment Processes, Micromobilization, and Movement Particpation,” *American Sociiological Review*, August 1986: 464–481.

[178] David Snow and Scott Byrd, “Ideology, Framing Processes, and Islamic Terrorist Movements,” *Mobilization: An International Quarterly Review*, 2000: 119–136.

[179] Arquilla and Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, 319.

[180] The use of the term “viral” to describe self-perpetuating successive or rolling operations against a web of connected actors, such as insurgents, is from Scott Swanson, “Viral Targeting of the IED Social Network System,” 12–14. Also, this concept has been characterized as “assault ‘till dawn” meaning there is one planned target captured, knowing that immediate results of on-site tactical questioning of the detained individual(s) leads immediately to the next wanted high-value individual, which the assault force then detains and interrogates, and does this again, and so on (from conversations with Special Operations planners and operators, 2004–2010). This is different from cascading network collapse which is applicable to technical systems like computer networks.

[181] Eric Walton, “The Persistence of Bureaucracy: A Meta-analysis of Weber’s Model of Bureaucratic Control,” *www.sagepublications.com.* 2005. http://oss.sagepub.com/cgi/content/abstract/26/4/569.

[182] Andrew Molnar, *Human Factors Considerations of Undegrounds in Insurgencies*, 20–26.

[183] Derived from Derek Jones, “Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations,” (Master’s thesis, U.S. Army School of Advanced Military Studies, 2009), 24–26, and Scott Swanson, “Viral Tareting of the IED Social Network System,” 2007, 4.

[184] Department of the Army. *FM 5–0 Army Planning and Orders Production* (Washington, D.C.: GPO, 2005), 3–42.

[185] Doug McAdam, “Recruitment to High-Risk Activism: The Case of Freedom Summer,” *The American Journal of Sociology* 92, no. 1 (1986): 64–90.

[186] Sam Green and Bill Seigel, “The Weather Underground,” San Francisco, CA: *The Free History Project*, KQED, and ITVS, 2003.

[187] International Crisis Group, “About Crisis Group.” *International Crisis Group* website. http://www.crisisgroup.org/en/about.aspx (accessed April 22, 2010).

[188] International Crisis Group, “Terrorism in Indonesia: Noordin’s Networks, Asia Report No 114,” (Jakarta/Brussels: ICG, 2006). http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/114-terrorism-in-indonesia-noordins-networks.aspx.

[189] Sean F. Everton, *Disrupting Dark Networks* (New York: Cambridge University Press, 2012), 33–38.

[190] Anderson, Kenneth. "U.S. Counterterrorism Policy and Superpower Compliance with International Human Rights Norms." *Fordham Internaitonal Law Journal* (2006), 455–484.

[191] Nancy Roberts and Sean F. Everton, "Strategies for Combating Dark Networks," *Journal of Social Structure 12*, 2012: 4–7.

[192] Everton, *Disrupting Dark Networks*, 33–38.

[193] U.S. Agency for International Development, "The Development Response to Violent Extremism and Insurgency," agency internal policy, Washington, D.C., 2011. http://transition.usaid.gov/our_work/.../VEI_Policy_Final.pdf.

[194] Department of the Army. *FM 3–05.130 Army Special Operations Unconventional Warfare (Washington, D.C.: GPO*, 2008), 1–2–1–3.

[195] Daniel Kolva, "Foreign Fighter Interdiction: Stability Operations as Countermeasures," *www.pksoi.army.mil.* April 1, 2011. http://pksoi.army.mil/PKM/publications/relatedpubs/documents/Kolva_Foreign_Fighters.pdf.

[196] School of Advanced International Studies Johns Hopkins University. "Academics-Conflict Management Toolkit-Approaches-Statebuilding-Insitution building," *www.sais-jhu.ed*, accessed September 20, 2010http://www.sais-jhu.edu/cmtoolkit/approaches/statebuilding/institution-building.htm.

[197] Department of the Army, *Field Manual 3–05.30 Psychological Operations* (Washington, D.C.: GPO, 2005), 1–2–1–3.

[198] Daniel Benjamin, "Remarks at first meeting of the Center of Excellence on Countering Violent Extremism." *www.state.gov.* January 25, 2012. http://www.state.gov/j/ct/rls/rm/2012/182716.htm (accessed September 30, 2012); Naureen Chawdhury Fink and Ellie B. Hearne, "Beyond Terrorism: Deradicalization and Disengagement from Violent Extremism," *International Peace Institute website.* October 2008. http://www.ipinst.org/publication/all-publications/detail/24-beyond-terrorism-deradicalization-and-disengagement-from-violent-extremism.html (accessed September 30, 2010).

[199] Department of the Army. *ADRP 2–0 Intelligence.* Fort Leavenworth, KS: U.S. Army Combined Arms Center, 2012., Glossary-4.

[200] Sean F Everton, *Disrupting Dark Networks*, 32–33.

[201] United Nations. "UN 1267 Committee Press Release." *United Nations website.* October 25, 2002. http://www.un.org/News/Press/docs/2002/SC7548.doc.htm.

[202] International Crisis Group, "Terrorism in Indonesia: Noordin's Networks," 19. The remainder of this chapter relies heavily upon this entire document. The derived datasets used in all measurements are also sourced from this same document.

[203] Photo taken from http://ravespot.wordpress.com/ "Indonesian court goes easy on Noordin's little helper." *Ravespot blog.* July 30, 2010. All network graphs inthis thesis were created usng UCINET 6.0, Borgatti, S.P., M.G. Everett, and L.C. Freeman. *UCINET 6.0 Version 6.411*. Natick: Analytic Technologies, 1999.

[204] International Crisis Group, "Indonesia: Noordin Top's Support Base, Asia Update Briefing No 29," Jakarta/Brussels: International Crisis Group, 2009. http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/B095-indonesia-noordin-tops-support-base.aspx.

[205] Van Der Merwe, Renier Hendrik. "Jemaah Islamiyah - Critical Discussion of Tactics and Threats." *www.newsblaze.com.* November 22, 2009. http://newsblaze.com/story/20091122185010iiis.nb/topstory.html (accessed September 20, 2010).

[206] Gordon, David, and Samuel Lindo. "Jemaah Islamiyah." *www.csis.org.* November 1, 2011. http://csis.org/publication/jemaah-islamiyah, 3.

[207] International Crisis Group, "Terrorism in Indonesia: Noordin's Networks," 3.

[208] Roberts and Everton, "Strategies for Combating Dark Networks," 19–20.

[209] International Crisis Group, "Terrorism in Indonesia: Noordin's Networks," 19.

[210] Carl Ungerer, "Jihadists in Jail: Radicalisation and the Indonesian Prison Experience," *www.aspi.org.au.* http://www.aspi.org.au/publications/publication_details.aspx?ContentID=293&pubtype=-1.

[211] See note 209 above.

[212] International Crisis Group, "Terrorism in Indonesia: Noordin's Networks," 27.

[213] Jefferson Mack, *The Safe House* (Boulder, CO: Paladin Press, 2008), 65–83.

[214] "Presidential Approval and Reporting of Covert Actions*."* *50 U.S.C. § 413b (2005).*

[215] United Nations Organization. "Chapter VII: Action with Respect to Threats to the Peace, Breaches or the Peace, and Acts of Aggression." *Charter of the United Nations.* June 26, 1945.

[216] Department of the Army. *FM 3–13 Information Operations: Doctrine, Tactics, Techniques, and Procedures.* Washington, D.C.: GPO, 2003., 1–14–1–17.

[217] Hassan, Muhammad Haniff. "Community-Based Initiatives against JI by Singapore's Muslim Community." *www.rsis.edu.sg.* January 16, 2006. www.rsis.edu.sg/publications/Perspective/IDSS0042006.pdf (accessed October 20, 2012).

[218] Use of symphony analogy borrowed from George Crile, *Charlie Wilson's War* (New York: Atlantic Monthly, 2003), 304.

[219] Gordon McCormick, unpublished class lecture notes, *SO3802 Seminar in Guerrilla Warfare*, January 2007.; "McCormick Magic Diamond," *www.wikipedia.org.* http://en.wikipedia.org/wiki/McCormick_Magic_Diamond (accessed October 20, 2010).

[220] Lawrence E. Cline, "Pseudo Operations and Counterinsurgency: Lessons from Other Countries." *www.strategicstudiesinstitute.army.mil.* June 1, 2005. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=607.

[221] Ibid., v–vi, 25–26.

[222] Ron Reid-Daly, *Pamwe Chete: The Legend of the Selous Scouts.* Johannesburg: Covos-Day Books, 2001.

[223] Cline, “Pseudo Operations and Counterinsurgency: Lessons from Other Countries,” 21–26.

[224] Nicholas Marschall, *Methodological Pitfalls in Social Network Analysis.* Saarbrucken, Germany: VDM Verlag Dr. Muller, 2007.

LIST OF REFERENCES

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network-Centric Warfare.* Washington, D.C.: GPO, 1999.

Alberts, David S., and Richard E. Hayes. *Power to the Edge: Command and Control in the Information Age.* Washington, D.C.: GPO, 2003.

Anderson, Kenneth. “U.S. Counterterrorism Policy and Superpower Compliance with International Human Rights Norms.” *Fordham International Law Journal*, 2006: 455–484.

Arquilla, John. *Worst Enemy: The Reluctant Transformation of the American Military.* Chicago: Ivan R. Dee Publishing, 2008.

Arquilla, John and David Ronfeldt. “Netwar Revisited: The Fight for the Future Continues.” In *Networks, Terrorism and Global Insurgency,* by Robert J. Bunker, 8–19. New York: Routledge, 2006.

Arquilla, John, and David Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Santa Monica, CA: RAND, 2001.

Baker, Wayne E., and Robert R. Faulkner. “The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry.” *American Sociological Review* 58 (1993): 837–860.

Ballester, Coralio, Antoni Calvo-Armengol, and Yves Zenou. “Who’s Who in Crime Networks. Wanted: The Key Player.” *Econometrica* 74 (2006): 1403–1417.

Barabasi, Albert-Laszlo. *Linked: How Everything is Connected*. New York: Plume, 2002.

Barabasi, Albert-Laszlo, and Eric Bonabeau. “Scale-Free Networks.” *Scientific American*, May 2003: 50–59.

Beam, Louis. “Leaderless Resistance.” *The Seditionist*, 12 (1992): 12–13.

Bell, J. Bowyer. *Dragonwars: Armed Struggle and the Conventions of Modern War.* London: Transaction Publishers, 1999.

———. *The Dynamics of the Armed Struggle.* London: Frank Cass Publishers, 1998.

Benjamin, Daniel. “Remarks at first meeting of the Center of Excellence on Countering Violent Extremism.” January 25, 2012.

Bienensock, Elisa Jayne, and Phillip Bonacich. "Balancing Efficiency and Vulnerability in Social Networks." Paper presented and collected in *Dynamic Social Network Modeling and Analysis: Workshop Papers*, 2003: 253–264.

Bonacich, Phillip. "Some Unique Properties of Eigenvector Centrality." *Social Networks* 29, no. 4 (2007): 555–564.

———. "Technique for Analyzing Overlapping Memberships." *Sociological Methodology* 4 (1972): 176–185.

Borgatti, Stephen. "Identifying Sets of Key Players in a Network." *Computational & Mathematical Organization Theory* , April 2006: 21–34.

———. *UCINET Software History*. https://sites.google.com/site/ucinetsoftware/history (accessed December 5, 2012).

Borgatti, Stephen, M.G. Everett, and Linton C. Freeman. *UCINET 6.0 Version 6.411*. Natick: Analytic Technologies, 1999.

Brafman, Ori, and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Penguin, 2006.

Bunker, Robert. "Introduction and Overview: Why Response Networks?" In *Networks, Terrorism and Global Insurgency*. New York: Routledge, 2006, 1–7.

Burges, Lisa. "Iraq War: Special Forces Followed up on Afghanistan Success." *Stars and Stripes*, May 27, 2003, http://www.stripes.com/news/iraq-war-special-forces-followed-up-on-afghanistan-success-1.6044.

Burt, Ronald. *Structural Holes: The Social Structure of Competition.* Cambridge: Harvard University Press, 1992.

Carley, Kathleen, "Dynamic Network Analysis for Counter-Terrorism," University of Illinois Urbana-Champagne. doi: 10.1.1.137.9475.

Carley, Kathleen, Jana Diesner, Jeffrey Reminga, Maksim Tsvetovat., "An Integrated Approach to the Collection and Analysis of Network Data," Paper presented at the NAACSOS 2004 Conference, http://www.casos.cs.cmu.edu/events/conferences/2004/2004_proceedings/Carley_Diesner_Reminga.pdf.

Carley, Kathleen M., Ju-Sung Lee, and David Krackhardt. "Destabilizing Networks." *Connections*, 2002: 79–92.

Carley, Kathleen, Jeffrey Reminga and Steve Borgatti. “Destabilizing Dynamic Networks Under Conditions of Uncertainty.” Paper presented at International Conference on Integration of Knowledge Intensive Multi-Agent Systems, 30 Sept.–4 Oct. 2003. 121–126, http://ieeexplore.ieee.org/iel5/8803/27847 /01245033.pdf?arnumber=1245033.

Carley, Kathleen M., and Yuqing Ren. *Tradeoffs Between Performance and Adaptability for C3I.* Interim paper, Pittsburgh: Carnegie Mellon University, 2001.

Cerami, Joseph R., and Jay W. Boggs, . *The Interagency and Counterinsurgency Warfare: Stability, Security, Transition and Reconstruction Roles.* Carlisle Barracks, Pennsylvania: U.S. Army Strategic Studies Institute, 2007.

Clausewitz, Karl Von. *On War.* Translated by Michael Elliot Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1989.

Cline, Lawrence E. “Pseudo Operations and Counterinsurgency: Lessons from Other Countries .” *www.strategicstudiesinstitute.army.mil*. June 1, 2005. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=607 (accessed April 15, 2008).

Connett, Ty, and Bob Cassidy. “Village Stability Operations: More than Village Defense.” *Special Warfare*, July-September 2011: 22–27.

Countering Violent Extremism Hearing Before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities. 111th Cong., 2nd sess. (2010). (testimony of LTG Francis H. Kearny, III).

Crile, George. *Charlie Wilson’s War.* New York: Atlantic Monthly Press, 2003.

Curtis, David. “How can we See Black Holes?” *Spacetime Wrinkles Exhibit* (1995).

de Nooy, Wouter, Andrej Mrvar, and Vladimir Batagelj. *Exploratory Social Network Analysis with Pajek.* Cambridge: Cambridge University Press, 2005.

Department of Defense. *Commander’s Handbook for an Effects-Based Approach to Joint Operations*. Washington, D.C.: GPO, 2006.

———. *JP 2–01.3 Joint Intelligence Preparation of the Operational Environment.* Washington, D.C.: GPO, 2009.

———. *JP 3–0 Joint Operations.* Washington, D.C.: GPO, 2011.

———. *JP 3–05.2 Joint TTPs for Special Operations Targeting and Mission Planning.* Washington, D.C.: GPO, 2003.

———. *JP 3–24 Joint Counterinsurgency*. Washington, D.C.: GPO, 2009.

———. *JP 3–60 Joint Targeting.* Washington, D.C.: GPO, 2007.

———. *JP 5–0 Joint Operation Planning.* Washington, D.C.: GPO, 2011.

———. "Unified Command Plan 2011." *www.defense.gov.* 2011. http://www.defense.gov/home/features/2009/0109_unifiedcommand/ (accessed December 2011)

Department of the Army. *ADRP 2–0 Intelligence.* Washington, D.C.: GPO, 2012.

———. *FM 3–0 Full Spectrum Operations.* Washington, D.C.: GPO, 2008.

———. *FM 3–05 Army Special Operations Forces.* Washington, D.C.: GPO, 2006.

———. *FM 3–05.130 Army Special Operations Unconventional Warfare.* Washington, D.C.: GPO, 2008.

———. *FM 3–05.20 Special Forces Operations.* Washington, D.C.: GPO, 2001.

———. *FM 3–05.201 Special Forces Unconventional Warfare (S//NF).* Washington, D.C.: GPO, 2007.

———. *FM 3–05.30 Psychological Operations.* Washington, D.C.: GPO, April, 2005.

———. *FM 3–13 Information Operations: Doctrine, Tactics, Techniques, and Procedures.* Washington, D.C.: GPO, 2003.

———. *FM 3–24 Counterinsurgency.* Washington, D.C.: GPO, 2006.

———. *FM 5–0. Army Planning and Orders Production.* Washington, D.C.: U.S. GPO, January, 2005.

———. *Special Forces Qualification Course 18A Course Student Curriculum Handout.* 1999.

———. *TRADOC Pam 525–5–500 Commander's Appreciation and Campaign Design.* Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2008.

Diani, Mario, and Doug McAdam. *Social Movements and Networks.* Oxford: Oxford University Press, 2003.

Dodson, John. "Man-hunting, Nexus Topography, Dark Networks and Small Worlds." *IO Sphere* (2006): pp. 7–10.

Doughty, Robert. *The Evolution of U.S. Army Tactical Doctrine, 1946–76.* Fort Leavenworth, KS: Combat Studies Institute, 2001.

Dozier, Kimberly. "Green Beret Equals Special Forces—Got it?" The Associated Press. November 17, 2011. http://www.boston.com/news/nation/washington/articles/2011/11/17/special_forces_equals_green_berets_got_it/.

———. "Petraeus Highlight Spec Ops Success in Afghanistan." *Fayetteville Observer*. Fayetteville Observer. Fayetteville, NC, September 4, 2011.

Emery, Norman. "Irregular Warfare Information Operations: Understanding the Role of People, Capabilities, and Effects." *Military Review*, November–December 2008: 27–38.

Erickson, Bonnie. "Secret Societies and Social Structure." *Social Forces* 60, no. 1 (1981): 188–210.

Everton, Sean F. *Disrupting Dark Networks.* Cambridge and New York: Cambridge University Press, 2012.

Faint, Charles, and Michael Harris. "F3EAD: Ops/Intel Fusion "Feeds" the SOF Targeting Process." *www.smallwarsjournal.com.* January 31, 2012. http://smallwarsjournal.com/jrnl/art/f3ead-opsintel-fusion-%E2%80%9Cfeeds%E2%80%9D-the-sof-targeting-process (accessed February 15, 2012).

Fink, Naureen Chawdhury, and Ellie B. Hearne. "Beyond Terrorism: Deradicalization and Disengagement from Violent Extremism." *International Peace Institute website.* October 2008. http://www.ipinst.org/publication/all-publications/detail/24-beyond-terrorism-deradicalization-and-disengagement-from-violent-extremism.html (accessed September 30, 2010).

Fischbeck, Paul, Matthew Dombroski, and Kathleen Carley. "Estimating Shape of Covert Networks," *Proceedings of the 8th International Command and Control Research and Technology Symposium,* Washington, DC., 2003.

Freeman, Linton. "Centrality in Social Networks Conceptual Clarification." *Social Networks*, 1979: 215–239.

Garfinkel, Simson L. "Leaderless Resistance Today." *FirstMonday* 8 (2003).

Gordon, David, and Samuel Lindo. "Jema'ah Islamiyah." *www.csis.org.* November 1, 2011. http://csis.org/publication/jemaah-islamiyah (accessed October 28, 2012).

Granovetter, Mark. “Economic Action and Social Structure: The Problem of Embeddedness.” *The American Journal of Sociology* 91, no. 3, (1985), 481–510.

———. “The Strength of Weak Ties.” *American Journal of Sociology*, 1973: 1360–1380.

———. “The Strength of Weak Ties: A Network Theory Revisited.” In *Social Structure and Analysis*, edited by P. Marsden and N. Lin. Beverly Hills, CA: Sage, 1982.

Green, Sam, and Bill Seigel. “The Weather Underground.” San Francisco, CA: The Free History Project, KQED, and ITVS, 2003.

Grimmet, Richard. “Instances of Use of United States Armed Forces Abroad, 1789–2009.” CRS Report, Congressional Research Service, Washington, D.C., 2010.

Gurteen, David. “On defining the problmen by Albert Einstein.” http://www.gurteen.com/gurteen/gurteen.nsf/id/L004680/.

Hammill, Jonathan T. “Analysis of Layered Social Networks.” PhD disseration, Air Force Institute of Technology, 2006.

Hanneman, Robert A., and Mark Riddle. *Introduction to Social Network Methods.* Riverside, CA: University of California, Riverside, 2005. http://faculty.ucr.edu/~hanneman/.

Hassan, Muhammad Haniff. “Community-Based Initiatives against JI by Singapore’s Muslim Community,” January 16, 2006. www.rsis.edu.sg/publications/Perspective/IDSS0042006.pdf (accessed October 20, 2012).

Hazelrigg, Lawrence E. “A Re-examination of Simmel’s ‘The Secret and the Secret Society’: Nine Propositions.” *Social Forces* 47 (1969): 323–330.

Herdt, Gilbert. “Secret Societies and Secret Collectives.” *Oceania* 60, no. 4 (1990): 360–381.

Holland, John H. *Hidden Order: How Adaptation Builds Complexity*. Cambridge, Perseus Books, 1995.

Hougham, Victoria. “Sociological Skills Used in Capture of Saddam Hussein.” *Footnotes* (2005).

“Divonis Mati Rois Bersyukur.” http://www.suaramerdeka.com/harian /0509/14/nas03.htm (accessed August 15, 2012).

Hunt, Richard. “The Challenge of Counterinsurgency.” *Second Indochina War Symposium.* Airlie, VA: Center of Military History U.S. Army Washington, D.C., 1986. 121–141.

“Indonesian court goes easy on Noordin’s little helper.” *Ravespot blog.* July 30, 2010.

International Crisis Group. “About Crisis Group.” *International Crisis Group website.* http://www.crisisgroup.org/en/about.aspx (accessed April 22, 2008).

International Crisis Group. “Indonesia: Noordin Top’s Support Base, Asia Update Briefing No29.” Jakarta/Brussels: International Crisis Group, 2009. http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/B095-indonesia-noordin-tops-support-base.aspx.

International Crisis Group. “Terrorism in Indonesia: Noordin’s Networks, Asia Report No 114.” Jakarta/Brussels: International Crisis Group, 2006. http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/114-terrorism-in-indonesia-noordins-networks.aspx

Joint Warfighting Center. *Commander’s Handbook for an Effects-Based Approach to Joint Operations.* Suffolk: U.S. Joint Forces Command, 2006.

Jones, Derek. “Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations.” *www.cgsc.edu.* May 2009. http://www.cgsc.edu/SAMS/media/Monographs/JonesD-21MAY09.pdf (accessed April 15, 2010).

Joseph Nye, Jr. *Soft Power: The Means to Success in World Politics.* New York: Public Affairs, 2004.

Kilduff, Martin, and Wenpin Tsai. *Social Networks and Organizations.* Thousand Oaks, CA: SAGE Publications, 2006.

Klerks, Peter. “The Network Paradigm Applied to Criminal Organizations.” *Connections* 24 (2001): 53–65.

Kolva, Daniel. “Foreign Fighter Interdiction: Stability Operations as Countermeasures.” *www.pksoi.army.mil.* April 1, 2011. http://pksoi.army.mil/PKM/publications/relatedpubs/documents/Kolva_Foreign_Fighters.pdf (accessed September 30, 2012).

Koschade, Stuart. “A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence.” *Studies in Conflict and Terrorism* 29 (2006) 559–575.

Krackhardt, David. “Simmelian Ties: Super Strong and Sticky.” In *Power and Influence in Organizations*, edited by Roderick Kramer and Margaret Neale, 21–38. Thousand Oaks, CA: Sage, 1998.

———. “The Ties That Torture: Simmelian Tie Analysis in Organizations.” *Research in the Sociology of Organizations*. 16 (1999): 183–210.

Krebs, Valdis. “Uncloaking Terrorist Networks.” FirstMonday 7, (2002): http://firstmonday.org/issues/issue7_4/krebs/index.html.

Krepinevich, Andrew F. *The Army in Vietnam.* Baltimore, MD: Johns Hopkins University Press, 1986.

Lamb, Christopher J., and Evan Munsing. *Secret Weapon: High-value Target Teams as an Organizational Innovation.* Washington, D.C.: NDU Press, 2011.

Lamb, Robert D. *Ungoverned Areas and Threats from Safe Havens.* Final Report of the Ungoverned Areas Project, Washington, D.C.: Office of the Secretary of Defense, 2007.

Leites, Nathan, and Jr., Charles Wolf. *Rebellion and Authority: An Analytical Essay on Insurgent Conflicts.* Chicago: Markham Publishing Co., 1970.

Lewin, Roger. *Complexity: Life at the Edge of Chaos*. New York: MacMillan Publishing Co, 1992.

Lugosky, Jena, and Rick Dove. “Understanding Stigmergy as a Pattern in Self-Organizing Adversarial Systems of Systems.” *www.parshift.com.* July 2011. http://www.parshift.com/s/110701AdversarialStigmergyPatterns-Essay.pdf (accessed April 15, 2012).

Mack, Jefferson. *The Safe House.* Boulder, CO: Paladin Press, 1998.

Mann III, Edward, Gary Endersby, and Thomas Searle. “Thinking Effects: Effects-based Methodology for Joint Operations.” *Cadre Paper No.15.* Mawell Air Force Base: Air University Press, 2002. 30.

Mann, Scott. “The Shaping Coalition Forces’ Strategic Narrative in Support of Village Stability Operations.” *www.smallwarsjournal.com.* 2011. http://smallwarsjournal.com/blog/journal/docs-temp/721-mann.pdf (accessed April 15, 2011).

Manwaring, Max. “The New Global Security Landscape: The Road Ahead.” In *Networks, Terrorism and Global Insurgency*, edited by Robert Bunker, 20–39. New York: Routledge, 2006.

Marschall, Nicholas. *Methodological Pitfalls in Social Network Analysis.* Saarbrucken, Germany: VDM Verlag Dr. Muller, 2007.

Mattis, James N. “USJFCOM Commander’s Guidance for Effects-based Operations.” *Parameters*, 2008: 18–25.

McAdam, Doug. *Political Process and the Development of Black Insurgency, 1920 - 1970.* 2nd Edition. Chicago: University of Chicago Press, 1999.

McAdam, Doug. “Recruitment to High-Risk Activism: The Case of Freedom Summer.” *The American Journal of Sociology* (The University of Chicago Press) 92, no. 1 (July 1986): 64–90.

McCormick, Gordon. “class lecture notes.” *SO3802 Seminar in Guerrilla Warfare.* unpublished, January 2007.

———. “McCormick Magic Diamond.” *www.wikipedia.org.* http://en.wikipedia.org/wiki/McCormick_Magic_Diamond (accessed October 20, 2010).

McFate, Montgomery. “Iraq: The Social Context of IEDs.” *Military Review* 85 (2005): 37–40.

McNeill, William. *The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000*. Chicago: University of Chicago Press, 1984.

Moffat, James. *Complexity Theory and Network Centric Warfare.* Washington, D.C.: DoD Command and Control Research Program, 2003.

Molnar, Andrew. *Human Factors Considerations of Undergrounds in Insurgencies.* Washington, D.C.: Special Operations Research Office, The American University, 1965.

Monge, Peter, and Noshir Contractor. *Theories of Communications Networks.* New York: Oxford University Press, 2003.

Murray, Williamson R., and Allan R. Millet. *Military Innovation in the Interwar Period*. New York: Cambridge University Press, 1996.

Nagaraja, Shishir, and Ross Anderson. “Topology of Covert Conflict.” University of Cambridge Computer Laboratory Technical Report. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-637.html

Naval Postgraduate School. *Codebook.* Unpublished, Department of Defense Analysis, Monterey, CA, 2008.

Newman, M. E. J. “The Mathematics of Networks.” *www-personal.umich.edu.* www-personal.umich.edu/~mejn/papers/palgrave.pdf (accessed August 20, 2009).

O’Connell, Robert L. *Of Arms and Men: A History of War, Weapons, and Aggression.* New York: Oxford University Press, 1989.

Osa, Maryjane. “Networks in Opposition: Linking Organizations Through Activists in the Polish People’s Republic.” In *Social Movements and Networks: Relational Approaches to Collective Action*, edited by Mario Diani and Doug McAdam. Oxford: Oxford University Press, 2003.

Peters, Ralph. “Constant Warfare.” *Parameters*, 1997: 4–14.

Phares, Walid. *The War of Ideas.* New York: Palgrave Macmillan, 2008.

“Presidential Approval and Reporting of Covert Actions.” *United States Code 50 (2005), sec. 413b.*

Raab, Jorg, and H. Brinton Milward. “Dark Networks as Problems.” *Journal of Public Administration Research and Theory* 13 (2003) 413–439.

Rabasa, Angel, et al. *Ungoverned Territories: Understanding and Reducing Terrorism Risks.* Research Report, RAND Project Air Force, Santa Monica, CA: RAND, 2007.

Reed, Brian. “A Social Network Approach to Understanding Insurgency.” *Parameters* (2007): 19–30.

Reid-Daly, Ron. *Pamwe Chete: The Legend of the Selous Scouts.* Johannesburg: Covos-Day Books, 2001.

Robb, John. *Brave New War*. Hoboken, NJ: John Wiley and Sons, Inc., 2007.

Roberts, Nancy, and Sean F. Everton. “Strategies for Combating Dark Networks.” *Journal of Social Structure* 12 (2012): 1–32.

Robinson, Linda. “Men on a Mission: U.S. Special Forces are Retooling for the War on Terror.” *www.usnews.com.* March 9, 2006. http://www.usnews.com/usnews/news/articles/060903/11shadow_print.htm (accessed April 15, 2008).

Rodrigues, Jose A. “The March 11th Terrorist Network: In its Weakness Lies its Strength.” Working paper, Department of Sociology and Analysis of Organizations, University of Barcelona, 2005.

Rosen, Stephen. *Winning the Next War: Innovation and the Modern Military*. New York: Cornell University Press, 1991.

Roseneau, James. "Many Damn Things Simultaneously." A paper presented at the Conference on Complexity, Global Politics, and National Security, sponsored by the National Defense University and the RAND Corporation, Washington, D.C., November 13, 1996. http://www.dodccrp.org/html4/bibliography/comch04.html.

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press, 2008.

Saxenian, Annalee. *Regional Advantage: Culture and Competition in Silicon Valley and Route 128*. Cambridge, MA: Harvard University Press, 1994.

Scarborough, Rowan. "Special Operations Forces Eye Terrorists." *The Washington Times.* Washington, D.C., August 11, 2005.

School of Advanced International Studies Johns Hopkins University. "Academics-Conflict Management Toolkit-Approaches-Statebuilding-Institution building." *www.sais-jhu.edu.* http://www.sais-jhu.edu/cmtoolkit/approaches/statebuilding/institution-building.htm (accessed September 20, 2010).

Schultz, Richard H., and Roy Godson. "www.weeklystandard.com." *www.weeklystandard.com.* July 31, 2006. http://www.weeklystandard.com/Content/Public/Articles/000/000/012/474cffnb.asp?pg=1 (accessed April 15, 2008).

Schultz, Richard, Robert Pfaltzgraff, and V. Bradley Stock, . *Roles and Missions for SOF in the Aftermath of the Cold War.* Diane Publishing, 1996.

Scott, John. *Social Network Analysis: A Handbook.* London: Sage Publications, 2005.

Simmel, Georg. *The Sociology of Georg Simmel.* Translated and edited by Kurt H. Wolff. New York: The Free Press, 1950.

Simmel, Georg. "The Sociology of Secrecy and of Secret Societies." *The American Journal of Sociology* XI, no. 4 (1906): 441–498.

Smith, Edward. *Complexity, Networking and Effects-Based Approaches to Operations.* Washington, D.C.: GPO, 2006.

Smith, Sir Rupert. *The Utility of Force: The Art of War in the Modern World.* New York: Vintage Books, 2008.

Snow, David, and Scott Byrd. “Ideology, Framing Processes, and Islamic Terrorist Movements.” *Mobilization: An International Quarterly Review*, 2000: 119–136.

Snow, David, E. Burke Rochford, Steven Worden, and Robert Benford. “Frame Alignment Processes, Micromobilization, and Movement Participation.” *American Sociological Review* (August 1986): 464–481.

Sparrow, Malcolm K. “The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects.” *Social Networks* 13 (1991): 251–274.

Stark, Rodney, and William Sims Bainbridge. “Networks of Faith: Interpersonal Bonds and Recruitment to Cults and Sects.” *American Journal of Sociology* 85, no. 6 (1980): 1376–1395.

Stockholm International Peace Research Institute. *SIPRI Year Book 2008: Armaments, Disarmaments and International Security*. SIPRI, Stockholm, Sweden: SIPRI, 2008.

Stompka, Piotr. *Trust: A Sociological Theory*. New York: Cambridge University Press, 1999.

Suara Merdeka. “Nasional-Divonis Mati Rois Bersyukur.” *www.suaramerdka.com*. September 14, 2005. http://www.suaramerdeka.com/harian/0509/14/nas03.htm (accessed September 20, 2011).

Sullivan, Michael. *How to Win and Know It: An Effects-Based Approach to Irregular Warfare*. Master’s thesis, Monterey, CA: Naval Postgraduate School, 2007.

Swanson, Scott. “Viral Targeting of the IED Social Network System,” May 2007. http://smallwarsjournal.com/documents/swjmag/v8/swanson-swjvol8-excerpt.pdf (accessed April 15, 2008).

Tarrow, Sidney. *Power in Movement: Social Movements and Contentious Politics*, 2nd ed. New York: Cambridge University Press, 1998.

Tilghman, Andrew. *Gates to Close JFCOM, Cut Gen. Officer Billets*. August 9, 2010. http://www.marinecorpstimes.com/news/2010/08/military_gates_cuts_080910w/ (accessed August 20, 2010).

Tovo, Ken. “From the Ashes of Phoenix: Lessons for Contemporary Counterinsurgency.” *Special Warfare*, January 2007: 7–15.

Treverton, Gregory F. *Intelligence, Law Enforcement and Homeland Security*. New York, 2002.

Tsvetovat, Maksim, and Kathleen Carley. “Bouncing Back: Recovery of Mechanisms of Covert Networks.” Paper presented at NAACSOS Conference Proceedings Pittsburgh, PA, 2003.

U.S. Congress. Senate. Armed Services Committee . “LTG Francis H. Kearny, III Countering Violent Extremism Testimony.” *www.armed-services.senate.gov*. March 10, 2010. armed-services.senate.gov/statemnt/2010/.../Kearney%2003–10–10.pdf (accessed April 15, 2011).

U.S. Agency for International Development. “The Development Response to Violent Extremism and Insurgency.” Agency Internal Policy, Washington, D.C., 2011. http://transition.usaid.gov/our_work/.../VEI_Policy_Final.pdf.

U.S. Library of Congress, Congressional Research Service, *Instances of Use of United States Armed Forces Abroad, 1798–2007*, by Richard F. Grimmett, CRS Report RL32170. Washington, DC: Office of Congressional Information and Publishing, January14, 2008.

Ungerer, Carl. “Jihadists in Jail: Radicalisation and the Indonesian Prison Experience.” *www.aspi.org.au.* May 19, 2011. http://www.aspi.org.au/publications/publication_details.aspx?ContentID=293&pubtype=-1 (accessed October 20, 2012).

United Nations Organization. “Chapter VII: Action with Respect to Threats to the Peace, Breaches or the Peace, and Acts of Aggression.” *Charter of the United Nations.* June 26, 1945.

United Nations. “UN 1267 Committee Press Release.” *United Nations website.* October 25, 2002. http://www.un.org/News/Press/docs/2002/SC7548.doc.htm (accessed April 15, 2008).

U.S. Army JFK Special Warfare Center and School. *Special Forces Qualification Course 18A Course Student Notes.* Fort Bragg, NC: U.S. Army JFK Special Warfare Center and School, 1999.

Van Der Merwe, Renier Hendrik. “Jemaah Islamiyah - Critical Discussion of Tactics and Threats.” *www.newsblaze.com.* November 22, 2009. http://newsblaze.com/story/20091122185010iiis.nb/topstory.html (accessed September 20, 2010).

Vandenbrouke, Lucien. *Perilous Options: Special Operations as an Instrument of Foreign Policy.* New York: Oxford University Press, 1993.

Waldrop, M. Mitchell. *Complexity: Emerging Science at the Edge of Order and Chaos*. New York: Simon and Schuster, 1992.

Walton, Eric. “The Persistence of Bureaucracy: A Meta-analysis of Weber’s Model of Bureaucratic Control.” *www.sagepublications.com.* 2005. http://oss.sagepub.com/cgi/content/abstract/26/4/569 (accessed April 15, 2010).

Wasserman, Stanley, and Katherine Faust. *Social Network Analysis: Methods and Explanations.* New York: Cambridge University Press, 1994.

Watt, Randy. “Action-Reaction-Counteraction.” *National Tactical Officers Association,* (Winter 2010): 46–48.

West, Nigel. “www.defensemedianetwork.com.” *www.defensemedianetwork.com.* June 1, 2010. http://www.defensemedianetwork.com/stories/international-special-operations-forces-2008–2009/ (accessed April 15, 2011).

Wiest, Dawn. “Story of Two Transnationalisms: Global Salafi Jihad and Transnational Human Rights Mobilization in the Middle East and North Africa.” *Mobilization,* (June 2007): 137–160.

Zell, Deone. “Social Network analysis and Knowledge Management.” *Docstoc.* USC, Fairfield, April 28, 2007. http://www.docstoc.com/docs/81260581/Social-Network-Analysis.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Office of the Assistant Secretary of Defense for Special Operations, Low-Intensity Conflict and Interdependent Capabilities
   ATTN: Mr. Timothy Strabbing
   Washington, DC

4. HQ, U.S. Special Operations Command
   ATTN: Headquarters Library
   MacDill AFB, FL

5. Commander, U.S. Army John F. Kennedy Special Warfare Center and School
   ATTN: LTC David C. Walton
   Ft. Bragg, NC

6. President, Joint Special Operations University
   ATTN: Dr. James D. Anderson
   MacDill AFB, FL

7. HQ, U.S. Special Operations Command
   ATTN: J7 Mr. Thomas M. Walton
   MacDill AFB, FL